CYBERSECURITY REQUIREMENTS

For the purposes of this Agreement, the North American Electric Corporation's Critical Infrastructure Protection (NERC CIP) requirements may impose mandatory language for some clauses. Notation is made where this is applicable.

Where notification is required within the terms of this Exhibit, such notification shall be made by telephone to the legal abbreviation Cyberthreat Operations Center (CTOC) at 816-701-0600. The CTOC is available 24 x 7, 365 days a year.

1. Supplier represents and warrants that:

   i. it continually adapts its software system development life cycle to adapt to emerging threats and vulnerabilities;

   ii. the SANS Top 25 Most Dangerous Programming Errors and/or the Open Web Application Security Project (OWASP) Top Ten identified vulnerabilities are integrated into its system development life cycle for software, system or Services provided to ESI or its affiliates;

   iii. the required third-party software and/or operating system security vulnerabilities are remediated prior to delivery of any software, systems, or services;

   iv. a security code review and/or or automated application security scan of Products is performed, and all identified security vulnerabilities are remediated prior implementation in the applicable environment; and

   v. any security vulnerabilities unable to be remediated must be mutually agreed and approved.

   vi. neither the system, software nor Services contain any back door, drop dead device, time bomb, Trojan horse, virus, or worm or any other code designed or intended to have, or capable of performing, any of the following functions:
      1. (i) disrupting, disabling, harming or otherwise impeding in any manner the operation of, or providing unauthorized access to, a computer system or network or other device on which such code is stored or installed; or
      2. (ii) damaging or destroying any data or file without the users' consent.

   vii. Supplier will provide capability to verify the identity of the software source for on premise software downloaded from Supplier. This term must be present for any Products or Services in scope for NERC CIP.

   viii. Supplier will provide the capability to verify the integrity of the software obtained for software installed on premise. This term must be present for any Products or Services in scope for NERC CIP.

   ix. Supplier will provide security patch information sufficient to evaluate applicability to software or systems. This term must be present for any Product or Services in scope for NERC CIP.

2. During the term of the parties' Agreement, if either party becomes aware of any vulnerabilities of the software, system, or Services, then such party shall promptly notify the other party. If such a

vulnerability is discovered and Supplier is notified of such discovery, then Supplier will prepare and present a vulnerability assessment to ESI within three (3) business days, without charge to ESI. Depending upon the results of the vulnerability assessment and the severity of the vulnerability, the parties shall work together on a reasonably acceptable remediation plan. Supplier will remediate any such discovered code vulnerabilities, including at a minimum, the SANS Top 25, the OWASP Top Ten, or a vulnerability confirmed by the United States Computer Emergency Readiness Team (US-CERT) according to the agreed upon remediation plan. This term must be present for any Products or Services in scope for NERC CIP.

3. Supplier represents and warrants that the software, system or Services will not limit ESI's ability to apply security-related patches, configuration changes, and upgrades to ESI computers hosting the software, system or Services. Patches, configuration changes, and updates to anti-malware Products include, but are not limited to, protection against any known or unknown malicious code and/or vulnerable security configurations.

Supplier Access to ESI Systems.

4. No access shall be given to Supplier except for that provided for through the parties' Agreement.

5. Supplier agrees to abide by applicable ESI's information policies while connected to ESI systems. Applicable policies are to be provided by ESI upon request. This term must be present for any Products or Services in scope for NERC CIP.

A. Remote Access.

i. All access will use a virtualized solution that is mutually agreed upon by both parties. If the solution is a Virtual Private Network (VPN), it shall not allow split tunneling.

ii. Supplier will only be granted access to the specific devices hosting its Products, and Supplier agrees to access only those specific devices.

iii. Level of access will be minimized based on required functions defined by the Agreement.

iv. Supplier will notify ESI immediately when remote access should no longer be granted to Supplier representatives. This term must be present for any Products or Services in scope for NERC CIP.

v. All requests for administrative access by Supplier must be mutually agreed upon and approved. If granted, rights will not extend beyond the specific system hosts applicable to the Agreement.

vi. Supplier will ensure that computers used at the remote end of any remote connection will have the latest available security patches applied to the operating system, browser, and/or application when accessing ESI's network and systems.

vii. Supplier will ensure that computers used at the remote end of any remote connection will have current anti-malware/virus software actively protecting the remote environment. Anti-malware/virus solution used by the Supplier must be a commercially-purchased Product.

B. Onsite Access.

i. ESI will assign a unique set of credentials to each individual employed by Supplier

requiring access to an ESI system.

ii. Supplier will forbid its employees from sharing any ESI login credentials.

iii. Supplier shall notify ESI within two (2) business days when there is any change in employment or position status of any of its ESI-credentialed staff performing services under the Agreement.

iv. Supplier will notify ESI immediately when onsite access should no longer be granted to Supplier representatives. This term must be present for any Products or Services in scope for NERC CIP.

v. If Supplier support requires the use of equipment not maintained by ESI, it will ensure that such equipment will adhere to the following standards before connecting to ESI systems:

a. Any computer system shall have the latest available critical security patches applied to the operating system, browser, and/or application.

b. The computer shall have current anti-malware/virus software actively protecting the remote environment. Anti-malware/virus solution used by the Supplier must be a commercially-purchased Product.

c. The Supplier agrees to allow ESI to perform any security-related scans deemed prudent by ESI before or while the computer is connected to ESI's network.

Data Protection.

6. Any transfer of ESI data outside of ESI systems shall include agreed upon security mechanisms, and at a minimum shall include encryption and authentication.

7. Supplier will not transfer data via removable media without authorization by a ESI member of Security management and not before a manual anti-virus scan is performed on the media. No data file will be transferred into ESI's network without being scanned for malicious code first. Any data that must be moved into or out of ESI's computing environment will be done via a secure file copy agreed to by ESI.

Security Incident.

8. For purposes of this Agreement:

"Company Data" means any and all non-public data originated by ESI including, but not limited to, data related to its finances, taxes, employees, customers, suppliers, shareholders, and business operations.

"Security Incident" means (i) any unauthorized use or disclosure of Company Data by Supplier or any of its affiliates or subcontractors; (ii) any unauthorized use or disclosure of Supplier's environment, Product or Service provided to ESI; and (iii) any unauthorized use or discloser of any third party development environment, Product or Services provided to ESI, and (iv) any reasonable belief that an unauthorized individual has accessed Company Data.

9. Supplier shall report, either orally or in writing, any Security Incident to ESI. Supplier shall make the report to ESI immediately upon discovery, but in no event more than two (2) business days after Supplier reasonably believes there has been or will be such Security Incident. Supplier's report shall identify: (i) the

nature of the unauthorized use or disclosure; (ii) the Company Data used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what Supplier has done or shall do to mitigate any Security Incident; and (v) what corrective action Supplier has taken or shall take to prevent future similar Security Incident. Supplier shall provide such other information, including a written report, as may be reasonably requested by ESI.

10. Supplier shall maintain security incident management policies and procedures, including detailed security incident escalation procedures. Supplier will initiate and coordinate orally or in written responses Supplier-identified incidents related to the Products or Services provided to ESI that pose a cyber security risk. This term must be present for any Products or Services in scope for NERC CIP.

11. Each party acknowledges that, in the course of performance of the Agreement, confidential and sensitive information that is transferred by ESI to Supplier Services/Infrastructure/Platform may be restricted by law from disclosure. Notwithstanding any other provision of the parties' Agreement to the contrary; Supplier, or any of its affiliates or subcontractors, will be responsible for all damages, fines, and corrective action arising from any security incident, breach of confidentiality and/or security of ESI data caused by Supplier, its officers, directors, employees, agents, representatives, contractors or others under its direction and control. The provisions of this clause shall supersede any term of the Agreement that conflicts with this provision.

Client Environment.

12. If access to Supplier's system, software or Services relies on third-party software installed on ESI's computers, Supplier agrees to maintain compatibility with the third-party software's critical security update schedule, at no charge to ESI. Supplier will provide updated Product to ESI within one (1) week of a third-party's notice of a flaw in software. If agreed upon in writing by both parties, the update schedule can be delayed.

Training.

13. The Supplier will provide periodic cyber security awareness training for its employees participating in the execution of any work under this Agreement.

Federal Regulation.

14. If applicable, Supplier agrees to assist ESI with compliance with federal regulatory requirements regarding information systems applying to system, software or Services defined in the Agreement.

Right to Audit: Oversight of Security Compliance.

15. ESI or its designated agent shall have the right to perform an assessment, audit, examination or review of all controls in Supplier's physical and/or technical environment in relation to the system, software or Services being provided to ESI pursuant to the Agreement to confirm Supplier's compliance with these terms, as well as any applicable laws, regulations and industry standards. Supplier shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and application software that processes, stores or transports information and data for ESI pursuant to the Agreement. In addition, upon ESI's request, Supplier shall provide ESI with the results of any audit by or on behalf of Supplier that assesses the effectiveness of Supplier's information security program as relevant to the security and confidentiality of information and data shared during the course of the Agreement.

The following additional terms apply when access by ESI or hosting of ESI data occurs outside of ESI systems. Examples include, but are not limited to, Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Hosted Environment.

16. If Supplier stores ESI information on a Supplier system (the "Hosted Environment"), Supplier agrees to maintain current anti-malicious code mechanisms for the environment it is hosting. Supplier will have a patch management program that keeps anti-virus/malware signatures updated as well as operating systems and any other software systems supporting the environment patched with regard to published security related vulnerabilities. Updates must be evaluated within one (1) week of publication of said patches/updates, and patches/updates deemed applicable must be implemented within one (1) month, unless a further delay is agreed upon by both parties. Published urgent critical patches are expected to be evaluated, and if deemed applicable, implemented in an expedited manner.

17. Supplier agrees to maintain secure configurations of its hosted environment with respect to emerging threats.

18. Access to Supplier's Hosted Environment requires authentication and encryption.

Data Processing & Storage - Ownership of and Access to Data.

19. Other than the rights and interests expressly set forth in the Agreement, ESI reserves all right, title and interest (including all intellectual property and proprietary rights) in data it provides to Supplier or ESI data which is otherwise in Supplier's possession or control. At ESI's sole discretion, ESI retains the right to access and retrieve its data stored outside of ESI systems on Supplier's system, software or Services infrastructure.

Disposition of Data.

20. Upon written request by ESI made before or within sixty (60) days after the effective date of termination or expiration, Supplier will make available to ESI a complete and secure (i.e., encrypted and appropriately authenticated) download file of ESI data in agreed format, or other format as reasonably requested by ESI.

21. On the expiration or termination of the Agreement or any applicable Statement of Work or Purchase Order, Supplier shall, at the choice of ESI securely return all ESI data transferred and all copies thereof to ESI, or shall securely destroy all the ESI data and certify in writing to ESI that it has done so, unless applicable law does not allow for the return or destruction of all or part of the data transferred. In that case, Supplier represents and warrants that it will ensure the confidentiality of the data transferred and will cease use and active processing of ESI data. ESI or its designated agent shall have the right to audit Supplier's data processing facilities for purposes of confirming compliance with the requirements set forth in this section.

Location of Data and Supplier Staff with Access to Data.

22. Supplier agrees to store and process ESI's data only in the continental United States. Supplier will limit remote access to ESI data to employees located in the continental United States or such other geographic location expressly agreed upon in writing by ESI.

Disaster Recovery.

23. Supplier has disaster recovery and business continuity mechanisms, processes, and responsibilities in place to ensure continuation of the contractually-agreed level of software, system or Services.

Vendor Outsourcing.

24. Supplier must identify to ESI any functionality that is outsourced, as well as the identity and the location of the outsourcing. Regardless of any such outsourcing, Supplier will remain directly responsible for all aspects of complying with the terms of the Agreement with ESI.

Legal/Government Requests for Access to Data

25. Where Supplier is required to disclose the confidential information of ESI pursuant to the order of a court or administrative body of competent jurisdiction or a government agency, Supplier shall (i) if practicable and permitted by law, notify ESI prior to such disclosure, and as soon as possible after such order; (ii) cooperate with ESI (at ESI's cost and expense) in the event that ESI elects to legally contest, request confidential treatment, or otherwise attempt to avoid or limit such disclosure; and (iii) limit such disclosure to the extent legally permissible.