DATA USE AGREEMENT

Attachment C

Security Controls

I. Personnel Controls

A. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DOM, or access or disclose DOM data must complete information privacy and security training, at least annually, at User's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

B. ***Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. ***Confidentiality Statement.*** All persons that will be working with DOM data must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DOM data. The statement must be renewed annually. The User shall retain each person's written confidentiality statement for DOM inspection for a period of six (6) years following contract termination.

D. ***Background Check.*** Before a member of the workforce may access DOM data, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with a more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The User shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

A. ***Workstation/Laptop/Tablet encryption.*** All workstations, tablets and laptops that process and/or store DOM PHI or PI must be encrypted using a FIPS 140-2 certified algorithm of 256 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DOM.

B. ***Server Security.*** Servers containing unencrypted DOM data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. **Co-Mingling of Data.** User agrees that all DOM data shall not be co-mingled with other trading partner's data, and shall be easily identifiable and exportable. DOM Data shall be stored in an individual structure in accordance with the following: User shall create an instance (single-tenant) of the particular database software utilized by User, and only DOM data shall reside in that instance of the database. The intent of this section is not to require separate procurement of hardware specific to DOM, however DOM data must not reside in a database that contains other entities' data.

D. ***Minimum Necessary.*** Only the minimum necessary amount of DOM data required to perform necessary business functions may be copied, downloaded, or exported.

E. ***Removable media devices.*** All electronic files that contain DOM data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, CDs/DVDs, Mobile Phones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm of 256 bit or higher, such as AES.

F. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DOM data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

G. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DOM data must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release. Applications and systems that cannot be patched due to operational reasons must have compensatory controls implemented to minimize risk, where possible.

H. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DOM data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours. User IDs shall be, purged after ninety (90) days of inactivity. Passwords are not to be shared. Passwords must be at least eight (8) characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every thirty (30) days. Passwords must conform to the following guidelines:

- Passwords must contain at least eight (8) characters.
- Passwords must contain a combination of lower case letters, upper case letters, numbers, and at least one (1) symbol.
- Minimum password age of 1 day.
- Maximum password age of 60 days.
- Enforce at least four (4) changed characters when new passwords are created.
- Prohibit password reuse for 24 generations.
- Passwords must not contain the user ID.
- Passwords must not include personal information about the user that can be easily guessed: user’s name, spouse’s name, kid’s name, employee number, social security number, birth date, telephone number, city, etc.
- Passwords must not include words from an English dictionary or foreign-language dictionary.
- Passwords must not contain any simple pattern of letters or numbers such as “qwertyxx”, “12345678”, or “xyz123xx.”

Two Factor Authentication (2FA) is preferred.

I. ***Data Destruction/Sanitization.*** DOM data in electronic form must be sanitized (cleared or purged) in accordance with NIST Special Publication 800-88 Rev.1 or as approved in writing by DOM. Media may also be physically destroyed in accordance with NIST Special Publication 800-88 Rev.1. User shall destroy all paper documents with DOM data by using a confidential method of destruction, such as crosscut shredding or contracting with a company that specializes in confidential destruction of document.

J. ***System Timeout.*** The system providing access to DOM data must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

K. ***Warning Banners.*** All systems providing access to DOM data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

L. ***System Logging*****.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DOM data, or which alters DOM data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DOM data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence.

M. ***Access Controls.*** The system providing access to DOM data must use role based access controls for all user authentications, enforcing the principle of least privilege.

N. ***Transmission encryption.*** All data transmissions of DOM PHI or PII outside the secure internal network must be encrypted using TLS 1.2 SHA-256 or higher encryption. This requirement pertains to any type of PHI or PII in motion including, but not limited to, website access, file transfer, and E-Mail.

O. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting DOM data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

A. ***System Security Review.*** User must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DOM data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools. A system risk assessment/security review must be done if a change to the boundaries of the system has occurred before the annual system risk assessment/security review is scheduled to be performed.

B. ***Log Reviews.*** All systems processing and/or storing DOM data must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing DOM data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

IV. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** User must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DOM data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

B. ***Data Backup Plan.*** User must have established documented procedures to backup DOM data to maintain retrievable exact copies of DOM data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DOM data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DOM data.

V. Paper Document Controls

A. ***Supervision of Data.*** DOM PHI or PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DOM PHI or PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. ***Escorting Visitors.*** Visitors to areas where DOM PHI or PII is contained shall be escorted and DOM PHI or PII shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** DOM data must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. ***Removal of Data.*** DOM data must not be removed from the premises of the User except with express written permission of DOM.

E. ***Faxing.*** Faxes containing DOM PHI or PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. ***Mailing.*** Mailings of DOM data shall be sealed and secured from damage or inappropriate viewing of PHI or PII to the extent possible. Mailings which include five hundred (500) or more individually identifiable records in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DOM to use another method is obtained.