RFP0292 - Exhibit 5

Information Security Requirements

Legal and general security requirements, access, and notifications

S-01 The contractor must comply with NYS Technology Law, including the Internet Security and Privacy Act, and will be responsible for any notifications required by Law. Any notifications must be approved by the AGM.

The Contractor and its personnel shall adhere to all required compliance domains, State security policies, procedures, and directives currently existing or implemented during the term of the Contract. ITS Policies may be found at the following web address: https://its.ny.gov/ciso/policies/security.

Specific to Security plan documentation, the Contractor shall complete the Consensus Assessment Initiative Questionnaire (CAIQ), on an annual basis and provide to AGM within 30 days of Assessment. At the sole discretion of AGM, AGM may accept other audited reports in lieu of the CAIQ, provided the report meets all other requirements in this section

In addition to a request for a CAIQ, the Contractor shall provide a written description of Contractor's physical/virtual security and/or internal control processes. At a minimum the Contractor's security documentation must contain the security activities listed below. These activities must be documented or referenced within an associated information security plan. Documentation must be sufficiently detailed to demonstrate the extent to which each security activity is applied. The documentation must be retained for auditing purposes.

The system must pass an internal NYS security review conducted by the New York State Office of Information Technology Services prior to implementation, and after any significant System modifications.

The purpose of the NYS security review is to determine whether adequate controls are in place to protect the availability of the System and the integrity and confidentiality of the information. It includes, but is not limited to:

- Description of the System including a listing of hardware and software;
- The sensitivity of data that is stored or transmitted;
- A diagram of the System including System components, data stores, and connections;
- Physical and logical vulnerabilities and associated security controls.

The Contractor must remediate all risks identified by the security assessment or obtain Authorized Users approval for compensating controls. The final outcome and Authorized Users approval of the security risk assessment must be documented and provided to the Authorized User.

S-02 Security incidents will require notification to AGM's authorized representative by phone within two hours of discovery. A written preliminary incident analysis report must be provided to AGM within 72 hours of discovery. Contractor representative must be available by phone and email for discussions with the NYS Cyber Command Center, ITS CISO, and AGM's Cyber Risk Coordinator throughout incident response activity and provide status updates at mutually agreed upon cadences. A written final incident analysis report, including a detailed technical section including root cause of incident, timeline, scope, impact, and corrective actions taken must be delivered to AGM at the conclusion of incident response.

Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:

1. notify the ITS CISO and any potentially affected Authorized User(s), or their designated contact person(s), by telephone as soon as possible, but in no event more than 12 hours from the time the Contractor confirms the Data Breach.

2. consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User;

3. coordinate all communication regarding the Data Breach with the ITS CISO and Authorized User (including possible communications with third parties);

4. cooperate with the Authorized User, ITS CISO and any Contractor working on behalf of the Authorized User or ITS CISO in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and

5. take such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide Written notice to the Authorized User as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if Contractor is unable to complete the corrective action within the required timeframe (i) the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

S-03 The Contractor is responsible for ensuring the solution complies with the most recent version of NYS Information Technology Policy, Information Security no. NYS-P03-002 and its associated policies and standards: https://its.ny.gov/eiso/policies/security

S-04 Access to AGM data must be restricted to those contractor employees with a need to access the information. The contractor will maintain a list of all its employees who have had access to AGM data, and supply this list to the AGM upon request.

S-05 AGM data may not be made available to any other person or organization except as described in this document and the contract or as otherwise authorized by the Department in writing.

S-06 Data encryption must meet or exceed the NYS Encryption Standard, NYS-S14-007, or successor. Personal identifiable information (PII) stored on the Contractor's system must be encrypted in

transit and at rest. For more information of which encryption to use, see the NYS ITS encryption standard, NYS-S14-007 https://www.its.ny.gov/document/encryption-standard

S-07 In the event that any part of the work is subcontracted, the contractor is responsible for all requirements identified in this document. Security logs and reports are expected to be available on demand.

Payment Card Requirements

S-08 The contractor is responsible for meeting the requirements of the current PCI-DSS merchant standards.

S-09 The contractor is responsible for maintaining the system to be compliant with PCI-DSS throughout the life of the contract.

S-10 The vendor will provide the AGM with documentation certifying compliance, and with a list of equipment in-scope for PCI-DSS upon request.

S-11 The vendor will hold harmless the AGM and NY State for any loss associated with a breach of data from the system.

Web based applications

S-12 Web based portions of the system must comply with NYS's Mandatory OFT Technology Policy NYS-P08-005, Accessibility of Web-Based Information and Applications, or be specifically approved for specific exceptions to this requirement in writing by AGM.

The contractor shall perform adequate testing on software applications used by AGM including, but not limited to security testing, unit testing, integration testing, regression testing, load testing, and user acceptance testing.

The contractor shall document and execute a remediation plan for any vulnerability identified through dynamic or static analysis, vulnerability scans or penetration tests.

The contractor or a qualified third party shall conduct vulnerability scanning against each proposed release of the Software. The contractor shall implement dynamic and static analysis in the software development environment to identify vulnerabilities.

The contractor shall provide the Executive Summary, including number of vulnerabilities and associated severity, from its most recent vulnerability scan and penetration test performed against the software application prior to the software going live.

Availability

S-13 The contractor must immediately notify the AGM verbally and via email upon learning of any situation expected to adversely affect the system usage, and of the anticipated downtime.

S-14 The contractor must submit a written description and a recommended resolution within three business days of learning of any situation expected to adversely affect the system usage.

S-15 The contractor must provide and maintain all hardware and software necessary to perform the required services. Unless otherwise agreed to by the AGM in writing, the contractor's current version of the software application must function as specified in the associated RFP in an environment comprised solely of components including, but not limited to operating system and database platform versions which are in an active support phase (e.g., no requirement to run on EOL life software such as Windows 7, etc.)

The contractor shall make commercially reasonable efforts to ensure that components including but not limited to third party libraries, components and APIs are maintained at their most recent, stable version within the released application made available to AGM.

S-16 The contractor must notify the AGM in writing of any scheduled system maintenance and what is being performed.

S-17 All system data will be the property of AGM and will be available to AGM in a usable electronic format upon request at no additional charges. Upon termination of the Contract, AGM shall have all access to data for a period of up to 60 days, and during this period, Contractor shall not take any action to erase or withhold any data, except as authorized or directed by AGM. After 60 days, Contractor shall destroy all AGM data and certify such destruction in writing. AGM has the right to withhold payment to contractor if AGM's data is not released to AGM as set forth herein.

S-18 The contractor will protect AGM data from access from any other customer or third party. The contractor should provide a Business Continuity and Disaster Recovery plan with stated service levels. This plan should meet the uptime required based on the NYS data classification. Data should be backed up regularly (several times a day).