

**AGGREGATE AGREEMENT UNDER IT MANUFACTURER
UMBRELLA CONTRACT #PM67350**

RFQ Title: New York State Law Enforcement Records Management System	RFQ #: 18-02
Contractor: Niche Technology Inc. 629 McDermot Avenue Winnipeg, MB R3A 1P6 Canada	
Contract #: PM67350	

THIS AGGREGATE AGREEMENT for the purchase of Law Enforcement Records Management System (RMS) Software and related Implementation Services for the New York State Police (“NYSP”) and other Authorized Users is made by and between the People of the State of New York, acting by and through the Commissioner of the Office of General Services (hereinafter “State” or “OGS”), with offices at the 41st Floor, Corning Tower, The Governor Nelson A. Rockefeller Empire State Plaza, Albany, New York 12242, and Niche Technology Inc., with offices at 629 McDermot Avenue, Winnipeg, MB R3A 1P6, Canada (hereinafter “Contractor”). The foregoing are collectively referred to herein as the “Parties.”

WHEREAS, OGS and Contractor are parties to Centralized Contract #PM67350 for Manufacturer Information Technology Commodities and Services; and

WHEREAS, pursuant to Contract #PM67350, Contractor is authorized to sell Software (Lot 1) and Implementation Services (Lot 4) to Authorized Users pursuant to the Request for Quote (RFQ) process set forth therein; and

WHEREAS, due to demand by Law Enforcement Agencies (LEAs) operating within New York State for RMS software and implementation services, OGS determined that the establishment, through the RFQ process, of an Aggregate Agreement with a Contractor offering modern, highly functional RMS software and implementation services at reasonable cost would serve the best interests of the State; and

WHEREAS, OGS issued an RFQ seeking RMS software and implementation services to all Contractors and their resellers under Award 22802 – Lots 1 and 4 on behalf of NYSP and Authorized Users who are Law Enforcement Agencies (LEAs) operating within New York State; and

WHEREAS, Contractor’s submission in response to the RFQ was evaluated, and OGS determined that the Contractor met all RFQ requirements and achieved the highest evaluation score from among all responding Contractors; and

WHEREAS, OGS and Contractor desire to enter into this Aggregate Agreement under Contract PM67350 to permit NYSP and other Authorized Users that qualify as Law Enforcement Agencies, as defined herein, to enter into Authorized User Agreements with Contractor to purchase Contractor's RMS software and implementation services.

NOW, THEREFORE, pursuant to the terms and conditions of Contract #PM67350 and in consideration of the terms and conditions set forth herein, the Parties do agree as follows:

SECTION 1. AGGREGATE AGREEMENT DOCUMENTS/ORDER OF PRECEDENCE.

This Aggregate Agreement is comprised of the following documents. Any conflicts or inconsistencies among such documents shall be resolved by giving precedence to the documents in the following order:

1. This document;
2. Attachment A, Pricing Pages, which consists of the Price Sheet as periodically approved by OGS;
3. Attachment B, Glossary of Terms, which contains definitions for certain terms in this Aggregate Agreement and its Attachments;
4. Attachment C, which consists of RFQ 18-02 Appendices 1 (Sample Forms), 2 (NYSP Volumes), 3 (Data Samples), 4 (SJS Overview), 5 (Data Structure Intel Case Management), 6 (E-ticket Accident Report Specification), and 7 (NY-gov ID Specifications);
5. Attachment D, How to Use. OGS reserves the right to unilaterally make revisions, changes and/or updates to Attachment D, How to Use without processing a formal amendment and/or modification to this Aggregate Agreement;
6. Contract PM67350 as in effect on the date of execution of this Aggregate Agreement, subject to OGS's Reserved Rights set forth in Section 8 below;
7. Attachment E, RFQ 18-02 Technical Response from the Contractor, which consists of the following documents, or portions thereof as indicated, from Contractor's response to RFQ 18-02:
 - RMS Attachment 1, Functional Requirements Niche Response *
 - RMS Attachment 2, Integration Requirements Niche Response *
 - RMS Attachment 3, System Requirements Niche Technology
 - RMS Attachment 4, Legacy Data Access Plan Niche Response *
 - RMS Attachment 5, Quality Management/Acceptance Testing Plan Niche Response*

- RMS Attachment 6, Support Plan Niche response *
- RMS Attachment 7, Project Plan Niche Technology (Personal Information redacted) *
- RMS Attachment 8, Training Plan Niche Technology*

*This response offered by the Contractor is a baseline for Plans and all the functionality of the RMS for all Authorized Users. The Contractor is bound by the baseline terms and conditions unless the Authorized User includes changes or additions in the Authorized User Agreement. Authorized Users may negotiate specific details in the Authorized User Agreement. Please see Attachment D, How to Use for further guidance.

8. Attachment F, Sales Report Form;
9. Attachment G, Agreement Modification Procedures; and
10. Attachment H, Contractor Information.

SECTION 2. AGGREGATE AGREEMENT TERM.

This Aggregate Agreement will take effect upon execution by Contractor and OGS and will have a term of five (5) years, contingent on an extension of the current term of Contract PM67350. In the event the current term of Contract PM67350 is extended, at OGS' option and upon notice to the Contractor, the five (5) year term of this Aggregate Agreement may be extended for a period ending 12 months beyond the new expiration date, or the termination date, whichever occurs first, of Contract PM67350.

Except as permitted below, Authorized User Agreements cannot extend 12 months past the expiration of Contract PM67350.

Lot 1 – Software

Pre-paid Maintenance/Support services within an Authorized User Agreement that is fully executed prior to the expiration of Contract PM67350 shall survive the expiration date of Contract PM67350 no longer than 60 months.

Lot 4 - Implementation Services

Authorized User Agreements fully executed prior to the expiration of Contract PM67350 shall survive the expiration date of Contract PM67350 based on the term of the Authorized User Agreement. An Authorized User Agreement for Lot 4, including any extensions, shall be no longer than 60 months in duration.

SECTION 3. LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEM ("RMS").

This Aggregate Agreement establishes a vehicle for Authorized Users to acquire a modern Law Enforcement Records Management System and related Implementation Services that will be an on-premise software solution as provided herein, at the prices specified herein. For the purposes of making an award, OGS used the New York State Police RMS project to establish an awarded Contractor, reasonableness of price and a price list. This Aggregate Agreement is considered an aggregate buy under Award 22802. Any Authorized User across New York State which meets the Attachment B, Glossary of Terms definition of a Law Enforcement Agency (LEA)¹ is authorized to execute Authorized User Agreements off this Aggregate Agreement to complete its separate RMS project. Subsequent purchases of software and services by Authorized Users other than the NYSP against this Aggregate Agreement may have different project requirements and deliverables unique to the Authorized Users. Such Authorized Users will need to prepare a Statement of Work containing any project-specific terms and conditions, timelines or standards required for the particular project.

Contractor shall not quote or charge Authorized Users pricing that exceeds the prices in Attachment A, Pricing Pages. This Aggregate Agreement is an Indefinite Delivery, Indefinite Quantity (IDIQ) award. There is no guarantee of the volume of business that Contractor may receive as a result of this Aggregate Agreement.

This Aggregate Agreement allows an Authorized User to implement a modern commercial off-the-shelf (COTS) RMS, with functionality including but not limited to:

- Documentation of Cases, investigations, calls for service, arrests and warrants (to include everything from a simple assist to a motorist, to conducting a complicated long-term homicide investigation)
- Providing the capability for Alerts, Flagging, and confidential investigations
- Providing robust Reporting capabilities
- Providing the capability to interface with multiple systems currently in use and those that may be added in the future (e.g. CAD, Livescan, NCIC/NLETS)
- Provide in-car access/Remote Access to the records management system with or without network connectivity
- A paperless Reporting system above the Station level
- Electronic Workflow - both for the submission of work and its return
- Providing robust search capabilities
- Extensive auditing capabilities

¹ A "Law Enforcement Agency" (LEA) is defined as any agency or department of the State, County, or local government which employs police officers as defined in Criminal Procedure Law section 1.20(34) OR has as its principal functions the prevention, detection or investigation of crimes; identification, apprehension, detention, prosecution, adjudication, or supervision of accused individuals, criminal offenders or other persons of interest; enforcement of the general criminal laws of the State; or crime analysis. Examples of State LEAs include NYSP and DEC. Examples of local LEAs include municipal police and county prosecutors.

- Electronically track property/evidence, allowing for the use of bar codes and interfacing with the Authorized User's laboratory information management systems
- Improve the safety of police officers and the public by providing investigative tools that enhance the ability of criminal justice agencies to navigate the criminal investigation process
- Improve efficiency and accuracy of data collection and provide users with advanced capabilities for Reporting, searching, and analyzing the data within the system
- Provide users of all levels of computer competency with a streamlined, easily navigable, and modern RMS that will aid in completion of their primary work objectives

SECTION 4. DEFINITIONS.

Definitions for certain terms in this Aggregate Agreement and its Attachments, can be found in Attachment B, Glossary of Terms.

SECTION 5. STATEMENT OF WORK.

5.1 Deliverables.

Deliverables shall be structured towards the goal of successful implementation of a fully functional RMS that can be tested and approved by the Authorized User.

For the purpose of this Aggregate Agreement, fully functional means the following:

- Containing the functionality as outlined in the Contractor's response in RMS Attachments 1 (Functional Requirements), 2(Integration Requirements), 3 (System Requirements), 4 (Legacy Data Access Plan) included in Attachment E; and
- The mechanism to access any legacy Data for the Records Management System has been successfully implemented and the software has been delivered, installed and accepted for the test and production systems; and
- Acceptance and performance testing have been completed to successful resolution, with all requirements proven, and agreed upon features and interfaces have been implemented; and
- The production system has been implemented and all Day 1 agreed upon RMS functionality have been transitioned to the new RMS. Day 1 functionality will be negotiated and agreed upon between the Contractor and the Authorized User.

The Contractor must work with the Authorized User to ensure that all the deliverables are met using standard NYS infrastructure elements and policies located in RMS Attachment 3, System Requirements (included in Attachment E) or as otherwise specified in the Statement of Work negotiated between the Authorized User and the Contractor. Additionally, the solution shall be in compliance with all CJIS security policies.

The deliverables may include, but are not limited to the following:

1. Contractor shall develop a detailed project schedule and project plans (staffing, communications, change management and risk management) based on best practices and obtain plan approval from the designated Authorized User Project Manager. At this time, the Contractor will provide the resume for its appointed Project Manager.
2. Contractor shall design and document the unit, integration and performance tests and obtain approval for each module from the designated Authorized User Project Manager, and complete successful installation of software in the development environment.
3. Contractor shall configure the application modules, build interfaces, execute the approved test plans for each module and obtain sign-off from the Authorized User Project Manager. This should include deployment of system ready for user acceptance testing and Authorized User acceptance of the training plan.
4. Following the successful completion of User Acceptance Testing of all modules, along with the acceptance of the results by the Authorized User Project Manager, Contractor shall coordinate and execute the implementation and stabilization of all application modules and interfaces that were agreed to during the project plan into the Authorized User's production environment.
5. Contractor shall successfully transfer application design, any additional code (i.e. interfaces) and operations knowledge to Authorized User staff (Train-the-trainer) and provide a support plan and obtain approval from the Authorized User Project Manager.
6. Contractor shall complete the implementation of a fully functional RMS.
7. In the 90 days after successful system implementation and Transition, Contractor shall repair all system defects to the satisfaction of the Authorized User.

5.2 Project Manager.

Unless otherwise directed by the Authorized User, the Contractor shall provide a full-time Project Manager dedicated to each Authorized User project. The Project Manager is an important resource to ensure project success. For the purposes of this Aggregate Agreement, the Project Manager shall be designated as key personnel and therefore must meet the following criteria and responsibilities:

- Criteria and responsibilities defined in the following Section, “Staffing Changes within Authorized User Agreement,” of Contract PS67350:

Staffing Changes within Authorized User Agreement.

1. Any staffing represented as key personnel are anticipated to fulfill the entire life of the project. If staffing changes are required for any of the key personnel on the project prior to the completion of his or her assignment period, the Contractor shall first, before proceeding with such removal, consult with and seek the approval of the Authorized User. If, after said consultation, it is mutually agreed that such removal shall take place, the Contractor shall provide the resumes of up to three (3) potential replacements with similar or better qualifications for the Authorized User review and approval within three (3) business days, or as otherwise agreed to by the Authorized User.
2. The newly-assigned Contractor staff must have qualifications as good as or better than those of the replaced staff. At the commencement of the transition period, the departing staff and the new staff will work together to develop a written transition plan to transition the responsibilities. The Authorized User reserves the right to approve this transition plan.
3. The Authorized User shall also have the right in its reasonable discretion to request removal of a Contractor Staff member at any time, and the Contractor must provide the resumes of up to three (3) potential replacements with similar or better qualifications for the Authorized User's review and approval within three (3) business days, or as otherwise agreed to by the Authorized User.
4. Where Contractor Staff ceases work for reasons beyond the control of the Contractor, the Contractor must immediately notify the Authorized User and provide the resumes of up to three (3) potential replacements with similar or better qualifications for the Authorized User's review and approval within three (3) business days, or as otherwise agreed to by the Authorized User.
 - a. Reasons beyond the control of the Contractor shall be defined as: (i) death of the Contractor Staff member; (ii) disability or illness; (iii) Contractor Staff member resigns his or her position; (iv) termination for cause by the Contractor; (v) military service or (vi) any other reason deemed acceptable by the Authorized User.
 - b. The provisions of this section do not preclude any Contractor Staff member from reasonable sick leave or annual leave.
5. Upon the Authorized User's approval, replacement staff will become project staff and will be subject to the terms and conditions of the Contract and Authorized User Agreement.

If the Authorized User does not approve one of the proposed replacement candidates, the Contractor must provide additional candidates for the Authorized User's review within three (3) business days. If the Authorized User still does not find a proposed replacement acceptable, the Authorized User reserves the right to either suspend activities under the Authorized User Agreement or terminate

the Authorized User Agreement for cause pursuant to Appendix B paragraph 47, Termination.

- The proposed Project Manager submitted by the Contractor shall have experience within the last five (5) years managing projects involving the implementation of law enforcement RMS. Two of those years must be with the Contractor's COTS RMS application.
- Unless otherwise specified in the Authorized User Agreement, the Project Manager shall be available during normal business hours (M-F, 8 AM-5 PM EST). The proposed schedule for the Project Manager will be approved by the Authorized User's Project Manager.
- Should a Contractor Staff member need to be replaced at any time, any associated cost will be borne by the Contractor.

SECTION 6. PRICING.

6.1 Attachment A, Pricing Pages.

Attachment A, Pricing Pages contains Aggregate Agreement Product pricing for Software licenses, Software maintenance and support and Implementation Services. Contractor shall not quote or charge Authorized Users pricing that exceeds the prices in Attachment A, Pricing Pages. Authorized Users are encouraged to request additional discounts at the time of a transaction.

The Product prices listed on Attachment A, Pricing Pages shall be all-inclusive and shall cover all shipping, handling, insurance, associated delivery charges, and all other costs. No other charges may be billed to an Authorized User including, but not limited to, processing or other fees for NYS Procurement Card purchases.

Aggregate Agreement Product discount percentage increases or Aggregate Agreement Product price decreases by the Contractor will be permitted at any time. Aggregate Agreement Product discount percentage decreases by the Contractor shall not be allowed and are specifically excluded from the terms and conditions of this Aggregate Agreement.

6.2 Enhancement to Services (Implementation).

When agreed to by the Authorized User, unanticipated enhancements to the services procured must not exceed a cumulative twenty (20) percent of the total Implementation Services cost. Any changes that will result in exceeding this twenty (20) percent will require that the Authorized User issue a new RFQ under Group 73600 – Award 22802 to procure the additional services. As project management is included within Lot 4, it is incumbent upon the Contractor to notify the Authorized User in writing when a requested scope change will exceed the cumulative twenty (20) percent total value of the Implementation Services of the project. Contractor's failure to do so may be deemed

a failure to manage the project and may be deemed a breach of the Authorized User Agreement.

6.3 Travel Costs.

As per the Contract PM67350 Section entitled “Travel, Meals, and Lodging – Lot 4 – Implementation Only,” travel is only allowed to be charged in connection with services provided out of Lot 4. Travel may be included as part of the Authorized User Agreement only up to that amount allowed by the travel guidelines outlined by the Office of the State Comptroller (OSC).

SECTION 7. AUTHORIZED USER TERMS AND CONDITIONS.

The following additional terms and conditions shall apply to all Authorized User Agreements executed from this Aggregate Agreement, in addition to any other terms and conditions specified by the Authorized User in the Authorized User Agreement.

7.1 No Removal of Records from Premises.

Where performance of the Contract involves use by the Contractor (or the Contractor’s subsidiaries, affiliates, partners, agents or subcontractors) of Authorized User owned or licensed papers, files, computer disks or other electronic storage devices, data or records at Authorized User facilities or offices, or via remote access, the Contractor (or the Contractor’s subsidiaries, affiliates, partners, agents or subcontractors) shall not remotely access, modify, delete, copy or remove such Records without the prior written approval of the Authorized User.

7.2 Contractor Staff.

This section shall supplement Section 42 of Appendix B to Contract PM67350.

For purposes of this section “Contractor Staff” includes all officers, agents, employees and subcontractors of the Contractor who shall perform Services under this Contract or have access to Authorized User Data.

All Contractor Staff shall possess the necessary qualifications, training, licenses, and permits as may be required within the jurisdiction where the Services specified are to be provided or performed and shall be legally entitled to work in such jurisdiction. All persons, corporations, or other legal entities that perform Services under the Contract on behalf of Contractor shall, in performing the Services, comply with all applicable Federal, State and local laws concerning employment in the United States.

All Contractor Staff shall, prior to the commencement of any Services on the project, whether on or off site, comply with all onboarding and security clearance requirements of the Authorized User, including any Public Safety agencies, and the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy

<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>) The Authorized User shall make all suitability determinations on Contractor Staff. For purposes of this Section, a “suitability determination” is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the State or the Authorized User. Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff, from performing any Services on this Project. All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable. If Contractor Staff are removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing Services under the Authorized User Agreement.

All Contractor Staff are also responsible for complying with all CJIS Policy requirements related to personnel including but not limited to Personnel Security and Security Awareness Training. All expenses, including travel and lodging associated with compliance of Contractor Staff to the CJIS Policy are the responsibility of the Contractor and are not reimbursable.

7.3 Nondisclosure, Confidentiality, Security and CJIS Compliance.

7.3.1 Nondisclosure And Confidentiality.

The following shall supplement the requirements of Section 9 (b) of Appendix B to Contract PM67350 – Confidential/Trade Secret Materials, Commissioner or Authorized User.

All Authorized User Data is owned exclusively by the Authorized User and will remain the property of the Authorized User for the sole use of performing an Authorized User Agreement issued under this Aggregate Agreement. Only the Authorized User or entities authorized in writing by the Authorized User will determine the terms and conditions of access to the Data. All Authorized User Data shall be considered Confidential Information subject to the terms of the resulting Authorized User Agreement and shall not be released to any third party without explicit written permission from the Authorized User’s Information Security Officer or designee.

Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, subcontractors, if any, shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors, if any, have access. The terms of this Section shall survive termination or expiration of this Aggregate Agreement. Contractor agrees that its officers, agents, employees, and subcontractors, if any, performing Services for the State and Authorized Users under this Aggregate Agreement shall be made aware of and shall agree in writing to the

terms of this Section. For purposes of this Aggregate Agreement, all State and Authorized User information of which Contractor, its officers, agents, employees, and subcontractors, if any, becomes aware during the course of performing Services for the Authorized User shall be deemed to be Confidential Information (oral, visual or written).

All information will be accounted for by the Contractor upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

The Contractor agrees that the Data processed during the performance of the Aggregate Agreement will be completely purged or destroyed in compliance with the CJIS sanitization and disposal standards section 5.8.3 and 5.8.4 (<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>) and the NYS Security Standard NYS-S13-003 for Sanitization/Secure Disposal (<https://www.its.ny.gov/eiso/policies/security>), or their successor policies, from all data storage components of the Contractor's computer facility and no output will be retained by the Contractor at the time the work is completed, except for the documents required to be maintained pursuant to paragraph 10 of Appendix A to Contract PM67350. If immediate purging of all data storage components is not possible, the Contractor will certify that any Data remaining in any storage component will be safeguarded to prevent unauthorized disclosures in accordance with FBI CJIS Security Policy.

The Contractor will be responsible for the destruction of any intermediate hard copy printouts and will provide the Authorized User Project Manager or his/her designee, with a statement containing the date of the destruction, description of material destroyed, and the method used. In the event that it becomes necessary for the Contractor to receive Confidential Information, which Federal or State statute or regulation prohibits from disclosure, the Contractor hereby agrees to return or destroy all such Confidential Information that has been received from the Authorized User when the purpose that necessitated its receipt by the Contractor has been completed. In addition, Contractor agrees not to retain any Confidential Information which Federal or State statute or regulation prohibits from disclosure after termination or expiration of the Aggregate Agreement, any Authorized User Agreement, and Contract PM67350.

Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, the Contractor agrees to extend the protections of this section and Contract PM67350 for as long as necessary to protect the Confidential Information and to limit any further use or disclosure of that Confidential Information by the Contractor. If Contractor elects to purge or destroy the Confidential Information, it shall be in compliance with the CJIS sanitization and disposal standards (<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>) and the NYS Security Standard NYS-S13-003 for Sanitization/Secure Disposal (<https://www.its.ny.gov/eiso/policies/security>) to achieve the same and notify the

Authorized User accordingly. The Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of the Authorized User's Confidential Information, which Federal or State statute or regulation prohibits from disclosure.

The Contractor shall never disclose information which Federal, State statute, or regulation prohibits from disclosure.

The Contractor agrees that it shall immediately report to the Authorized User as appropriate, the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information of the Authorized User information directly to the Authorized User's information security office.

It shall be a breach of the security of the system if Authorized User Confidential Information is disclosed to any unauthorized persons, including to agents, employees, officers, partners or subcontractors of Contractor who have not been authorized by the Authorized User to receive such Confidential Information. In the event of a breach of Confidential Information Contractor shall immediately notify the Authorized User information security office and, with the cooperation of the Authorized User or authorized designee, attempt to (i) determine the scope of the breach; and (ii) prevent the future recurrence of such security breaches.

Except as otherwise instructed by the Authorized User or authorized designee, upon the discovery of such breach Contractor shall first consult with and receive authorization from the Authorized User or authorized designee prior to notifying any parties to whom it is required to provide notice as prescribed by the New York State Information Security Breach and Notification Act of 2005 (ISBNA). Nothing herein shall in any way impair any authority of the New York State Attorney General to bring an action against Contractor to enforce the provisions of ISBNA. In the event of a breach of the security of the system (as defined by ISBNA) caused by Contractor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of Contractor's agents, officers, employees or subcontractors, Contractor shall be responsible for all costs associated with providing the notice required by the ISBNA.

Contractor shall hold the Authorized User and NY State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its officers, agents, employees, and subcontractors of such Confidential Information.

The Authorized User will have the right to terminate the Authorized User Agreement for cause if the Contractor fails to provide the safeguards described above or it is determined that the Contractor has violated a material term of this Section.

Notwithstanding the language contained in this Section, the Contractor may release any information pursuant to a final order issued from a Court of competent jurisdiction, provided the State, or other Authorized User, as applicable has had an opportunity to be heard.

Notwithstanding the foregoing, information which falls into any of the following categories shall not be considered Confidential Information:

- a. Information that is previously rightfully known to the receiving party without restriction on disclosure;
- b. Information that becomes, from no act or failure to act on the part of the receiving party, generally known in the relevant industry or is in the public domain;
- c. Information that is independently developed by the Contractor without use of Confidential Information of the Authorized User;
- d. Information unrelated to the scope of this engagement; and
- e. Information that the Authorized User has approved for disclosure, but solely in accordance with the Authorized User's approval or direction.

In addition to the foregoing, the Authorized User reserves, on its own behalf, the right in its discretion to require individual Contractor or subcontractor staff to execute Nondisclosure Agreements.

The provisions regarding Confidentiality and Disclosure shall survive Contract termination or expiration.

7.3.2 **Security.**

The following shall supplement the requirements of Section 56 of Appendix B to Contract PM67350:

Contractor agrees to preserve the confidentiality, integrity and accessibility of Authorized User Data with administrative, technical and physical measures that conform to federal, State and Authorized User mandates, and generally recognized industry standards and practices, to include the National Institute of Standards and Technology (NIST) 800-53 guidelines for implementing system security and privacy controls. Accordingly, Contractor must comply with State security policies and procedures, including but not limited to:

- Acceptable Use of Information Technology Resources Policy
- Information Security Policy
- Security Logging Standard
- Information Security Risk Management Standard
- Information Security Controls Standard
- Sanitization/Secure Disposal Standard
- Mobile Device Security Standard

- Remote Access Standard
- Secure System Development Life Cycle Standard
- Secure Configuration Standard
- Secure Coding Standard

ITS Security Policies and Standards may be found at
<http://www.its.ny.gov/tables/technologypolicyindex.htm/security>

7.4 Compliance with State & Federal Laws, Rules, Regulations, and Policies.

Contractor must also comply with State and Federal laws, rules, regulations, and policies, as well as all State and Authorized User policies regarding compliance with various confidentiality and privacy laws, rules and regulations, including but not limited to NYS Technology Law, Health Insurance Portability and Accountability Act (HIPAA); the Health Information Technology for Economic and Clinical Health Act (HITECH); IRS Publication 1075; Code of Federal Regulations, Title 42: Public Health, Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records; Family Educational Rights and Privacy Act (FERPA); the federal Driver's Privacy Protection Act of 1994 (DPPA); the Criminal Justice Information Services (CJIS) Security Policy during the performance of the Aggregate Agreement and any Authorized User Agreement t.

The Contractor must review the minimum-security requirements in RMS Attachment 3, System Requirements (included in Attachment E), any additional security requirements specified by an Authorized User, as well as the CJIS security policy requirements (<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>) and be able to provide a solution which prevents gaps in the secure operation of the proposed solution.

The following shall supplement the requirements of Section 61 of Appendix B to Contract PM67350, Indemnification: Contractor shall hold the State and the Authorized User harmless from any loss or damage to the State or the Authorized User resulting from the violation by the Contractor, its officers, agents, employees, and/or subcontractor, if any, of such security procedures or policies and from any criminal acts committed by such officers, agents, employees, and/or subcontractor, while providing Services under the Aggregate Agreement. For New York State Agency LEAs, the proposed solution may be housed at a New York State Data Center. Authorized User may monitor and control access to the proposed solution. The licensed product may be accessed after authentication is granted from the Authorized User's Security layer.

7.4.1 Specific Security Procedures.

In addition to compliance with the above specified policies the Contractor shall implement the following specific security procedures:

7.4.1.1 Data Location and Access.

It is the intent of this Aggregate Agreement that any Data related to this Aggregate Agreement reside on the premise of the Authorized User. There may be situations which necessitate the Data to be accessed or reside within the Contractor's environment on a temporary basis strictly to perform system configuration, maintenance and support. When these situations arise, and upon written approval of the Authorized User and in compliance with all applicable security procedures and policies of the Authorized User, the Contractor may access the Data from within their environment or store Authorized User Data in their environment. In all instances the Contractor must ensure that all Data related to the work performed pursuant to the project is accessed from or stored in a physically secure location or controlled area to ensure data security, confidentiality and integrity.

Notwithstanding the above Authorized User approval requirements, all access to, or storage of Data, whether physical or virtual, must be performed from within the Continental United States. The Contractor shall not send or permit to be sent, or store to any location outside of the Continental United States, any Data related to this project. Contractor shall provide to the Authorized User a list of the physical locations where the Data is stored at any given time and will update that list if the physical location changes. Adequate security systems, in compliance with all Authorized User policies and CJIS must be in place to control access into the facilities. Access into and within the facilities must be restricted through an access control system that requires positive identification of authorized individuals as well as maintains a log of all accesses as outlined in CJIS Security Policy. The Contractor shall have a formal procedure in place for granting computer system access to the Data and to track access. Access for projects outside of those approved by the Authorized User is prohibited.

7.4.1.2 Data Transport.

The Contractor shall use reputable means to transport Data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the Authorized User.

7.4.1.3 Data Protection.

The Contractor shall use appropriate means to preserve and protect Data related to this project. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. The Contractor must, in accordance with applicable law and the instructions of the Authorized User, maintain such Data for the time period required by applicable law, exercise due care for the protection of Data, and maintain appropriate data integrity safeguards against the deletion or alteration of

such Data. In the event that any Data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of this Aggregate Agreement and any Authorized User Agreement, then Contractor shall, at its own expense, use its best efforts to reconstruct such Data as soon as feasible. In such event, Contractor shall reimburse the Authorized User for any costs incurred by the Authorized User in correcting, recreating, restoring or reprocessing such Data or in providing assistance therewith.

Contractor agrees that any and all Authorized User Data will be stored, processed and maintained solely on designated target devices, and that no Authorized User Data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that device or storage medium is a necessary and approved component of the authorized business processes covered in the Authorized User Agreement, or the Contractor's designated backup and recovery processes, and is encrypted in accordance with all current federal and State statutes, regulations and requirements, to include requirements for Data defined as confidential, financial information, personal private and sensitive information (PPSI), personally identifying information (PII) or personal health information (PHI) by statute or regulations. The Contractor shall encrypt Data at rest, on file storage, database storage, or on back-up media, and in transit in accordance with state and federal law, rules, regulations, and requirements. The solution shall provide the ability to encrypt Data in motion and at rest in compliance with state or federal law.

7.4.1.4 Data Transmission.

Contractor shall use secure means (HTTPS) for all electronic transmission or exchange of system, user and application Data with the State.

7.4.2 Security Audits.

Contractor may be asked to provide a recent independent audit report on security controls prior to formal awarding of any Authorized User Agreement under this Aggregate Agreement or at any time during the Aggregate Agreement term. The Authorized User and any regulatory authority having jurisdiction over the Authorized User shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations used in the performance of any work under any Authorized User Agreement. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with this Aggregate Agreement or any Authorized User Agreement safeguards.

7.4.3 Secure Software.

The Contractor shall agree to maximize the security of the RMS solution throughout the term of this Aggregate Agreement as it applies to development, test and production environments (if under Contractor's or their agent's control) and agrees to take all necessary steps to ensure that developed software is safe, stable, and secure.

The Contractor agrees to maximize the security of the Software according to the following terms:

7.4.3.1 Protection.

The Contractor shall take all necessary actions to protect information regarding security issues and associated documentation, to help limit the likelihood that vulnerabilities in the software are exposed.

7.4.3.2 Standard.

The Contractor shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. The "highest applicable industry standards" shall be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

7.4.3.3 Security Training.

The Contractor represents and warrants that all members of their development team have been trained in secure programming techniques.

7.4.3.4 Vulnerabilities, Risks and Threats.

The Contractor shall use its best efforts to identify vulnerabilities, risks, and threats as early as possible during the software lifecycle. The software lifecycle shall mean from development, management, updates through retirement of the RMS solution.

The Contractor shall identify the key risks to the important assets and functions provided by the RMS solution. The Contractor shall conduct risk assessment(s) to assess and prioritize risks, enumerate vulnerabilities, and quantify the impact that particular attacks might have on the RMS solution. Such risk assessments will be used to ensure that the application meets applicable contractual obligations, regulatory mandates, and security best practices and standards.

The Contractor shall provide the Authorized User with written documentation of all security-relevant information regarding the vulnerabilities, risks, and threats to the RMS solution. Such security documentation shall be provided within a reasonable time based on the risk and upon identification of such vulnerabilities, risks, and threats and shall describe security design, risk analysis, and mitigation strategies.

7.4.3.5 Application Development.

Prior to commencing work under any Authorized User Agreement under this Aggregate Agreement, the Contractor shall provide the Authorized User written documentation detailing its application development, patch management, and update process. The documentation shall clearly identify the measures that will be taken at each level of the process to develop, maintain, and manage the software securely and include a written description of the industry security standards and standard of care followed in its application development, patch management, and update process and any additional security standards and level of care that must be implemented during the term of the Authorized User Agreement.

The Contractor shall provide secure configuration guidelines in writing to the Authorized User. These guidelines shall fully describe all security relevant configuration options and their implications for the overall security of the RMS solution. The guidelines shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured to maximize security. The default configuration of the software shall be secure.

7.4.3.6 Development Environment.

1. Configuration Management. The Contractor shall use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
2. Distribution. The Contractor shall use a build process that reliably builds a complete distribution from source. This process shall include a method for verifying the integrity of the software delivered to the Authorized User.
3. Disclosure. The Contractor shall document, in writing, to the Authorized User all third party software used in the application, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.
4. Evaluation. The Contractor shall make reasonable efforts to ensure that third party software meets all the terms of this Aggregate Agreement and any Authorized User Agreement and is as secure as custom developed code developed under this Aggregate Agreement and any Authorized User Agreement.

7.4.3.7 Testing.

1. General. The Contractor shall provide and follow a security test plan that defines an approach for testing or otherwise establishing that each of the security requirements has been met. The level of rigor of this test process shall be detailed in the plan. The Contractor shall implement the security test plan and provide the test results to the Authorized User in writing.
2. Source Code. The Contractor agrees that the source code shall be evaluated during the application development lifecycle process to ensure that the requirements of this Aggregate Agreement and any Authorized User Agreement, including the security standards, policies and best practices, are followed. The Contractor shall have a well-documented procedure and framework for conducting code reviews.
3. Vulnerability Scanning and Penetration Testing. The Contractor agrees that, before any Software is released to the Authorized User, the Contractor will perform application vulnerability scanning and penetration testing.

The Contractor shall provide to the Authorized User written documentation of the results of any scans and tests along with a mitigation plan.

The Contractor agrees that vulnerabilities identified by the vulnerability scanning and penetration testing shall be mitigated within a reasonable period of time to avoid any risk to the Authorized User.

7.4.3.8 Patches and Updates.

The Contractor shall provide notification of patches and updates affecting security within a pre-negotiated period as identified in the patch management process throughout the software lifecycle.

The Contractor shall apply, test, and validate the appropriate patches and updates and/or workarounds on a test version of the application before distribution.

The Contractor shall verify and provide written documentation that all updates have been tested and installed.

The Contractor shall verify application functionality, based upon pre-negotiated procedures, at the conclusion of patch updates, and provide documentation of the results.

7.4.3.9 Tracking Security Issues.

The Contractor shall track all security issues uncovered during the entire software lifecycle, whether it is a requirement design, implementation, testing,

deployment, or operational issue. The risk associated with each security issue shall be evaluated, documented, and reported to the Authorized User as soon as possible after discovery.

7.4.3.10 Delivery of the Secure Application.

The Contractor shall provide a "certification package" consisting of the security documentation created throughout the development process. The package shall establish that the security requirements, design, implementation, and test results were properly completed, and all security issues were resolved appropriately.

The Contractor shall fix all security issues that are identified before delivery. Security issues discovered after delivery shall be remediated in accordance with the NYS Standard on Vulnerability Scanning NYS-S15-002, (<https://www.its.ny.gov/eiso/policies/security>) to avoid any risk to the Authorized User.

7.4.3.11 Self-Certification.

The Contractor's Security Lead shall certify to the Authorized User, in writing, that the application meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status shall be fully documented with the delivery.

7.4.3.12 Independent Review.

The Authorized User reserves the right to perform its own independent application security review in addition to the Contractor Self-Certification.

7.4.3.13 No Malicious Code Warranty.

Contractor warrants that the RMS solution shall not contain any code that: (a) does not support a software requirement; or (b) weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

7.4.3.14 Security Acceptance and Maintenance.

1. Acceptance. The application shall not be considered accepted by the Authorized User until the Contractor certification package is complete and all security issues have been resolved.
2. Investigating Security Issues. After acceptance, the Authorized User reserves the right to perform Vulnerability Scanning and Penetration Testing at any time during the term of the Authorized User Agreement, if security

issues are discovered, by either Party, or reasonably suspected, Contractor shall assist the Authorized User in performing an investigation to determine the nature of the issue. Security issues discovered after acceptance shall be remediated in accordance with the NYS Standard on Vulnerability Scanning NYS-S15-002 (<https://www.its.ny.gov/eiso/policies/security>).

7.4.3.15 Source Code Escrow for Licensed Product.

At the request of the Authorized User, Contractor shall either: (i) provide Licensee with the Source Code for the Product; or (ii) place the Source Code in a third party escrow arrangement with a designated escrow agent who shall be named and identified to the Authorized User, and who shall be directed to release the deposited Source Code in accordance with a standard escrow agreement acceptable to the Authorized User; or (iii) will certify to the Authorized User that the Product manufacturer/developer has named the Authorized User, and the Licensee, as a named beneficiary of an established escrow arrangement with its designated escrow agent who shall be named and identified to the Authorized User and Licensee, and who shall be directed to release the deposited Source Code in accordance with the terms of escrow. Source Code, as well as any corrections or enhancements to such source code, shall be updated for each new release of the Product in the same manner as provided above and such updating of escrow shall be certified to the Authorized User in writing. Contractor shall identify the escrow agent upon commencement of the Contract term and shall certify annually that the escrow remains in effect in compliance with the terms of this clause.

The Authorized User may release the Source Code to Licensees under this Aggregate Agreement or any Authorized User Agreement who have licensed Product or obtained services, who may use such copy of the Source Code to maintain the Product.

7.4.4 CJIS.

Contractor is permitted to use Criminal Justice Information (CJI) solely for the purposes of performing the services as described in the Authorized User Agreement, and for no other purpose. At no time shall the Contractor access any criminal justice information (including criminal history record information or other sensitive criminal justice information) as defined by CJIS Security Policy, contained on Authorized User systems or media without complying with this section. Any access to computer media/systems which contain criminal justice information including criminal history record information and other sensitive criminal justice information is subject to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, specifically the Security Addendum (SA). (<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>)

The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal justice information (including criminal history record information), limits the use of the information to the specific purposes for which it is being provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, provides for sanctions, and contains such other provisions as required by the FBI Director.

The Contractor, as a condition precedent for providing Project Services for the benefit of the Authorized Users, and as evidenced by the Contractor signing this Aggregate Agreement, agrees:

(1) to abide by the SA, and (2) to the incorporation by reference of the SA as a part of this Aggregate Agreement and any Authorized User Agreement, (3) that the SA shall be incorporated by reference as a part of all subcontracts entered into by the Contractor the purpose of which is of the delivery of Project Services, if any; and (4) that those Contractor employees and subcontractor employees (Contractor Staff), if any that provide Project Services shall sign the form entitled, "Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification" as set forth in RFQ, (<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>)

One copy of the signed form will be retained by the Contractor and the original will be provided to the Authorized User for retention by the Authorized User's CJIS Information Security Office.

The Authorized User may terminate the Authorized User Agreement if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any and agents shall be made aware of and shall agree to the terms of this section.

7.5 Project Engagement Payment Schedule. *

The Contractor shall be paid in accordance with the total proposed project cost, excluding maintenance costs, identified in the Authorized User Agreement. For the purposes of the below payment schedule, total proposed project cost excludes maintenance cost as identified in the Authorized User Agreement documents. Maintenance costs shall be paid to the Contractor in the year maintenance is performed or in accordance with the terms agreed to with the Authorized User. The percentages of the total proposed project cost, which will be paid to the Contractor after acceptance by the Authorized User of each completed deliverable, shall be as follows:

- 10% of the total proposed project cost (excludes maintenance cost) shall be payable after delivery and acceptance of project management plans (project schedule,

staffing management, risk management, change management, communication plans)

- 10% of the total proposed project cost (excludes maintenance cost) shall be payable after successful installation of Software in Development Environment for configuration and delivery and acceptance of test plan
- 10% of the total proposed project cost (excludes maintenance cost) shall be payable after deployment of system ready for user acceptance testing and acceptance of training plan
- 10% of the total proposed project cost (excludes maintenance cost) shall be payable after any completed interfaces agreed to during the project plan
- 10% of the total proposed project cost (excludes maintenance cost) shall be payable after any required training is complete
- 30% of the total proposed project cost (excludes maintenance cost) shall be payable after successful system implementation and Transition
- 20% of the total proposed project cost (excludes maintenance cost) shall be payable 90 days after successful system implementation and Transition and all system defects have been repaired to the satisfaction of the Authorized User.

* Authorized User reserves the right to adjust this payment schedule in the Authorized User Agreement executed with the Contractor.

7.6 Software Maintenance and Support Fees.

Per Section 59 of Appendix B to Contract PM67350, there shall be a warranty period of 365 calendar days for all Authorized User Agreement Projects. The first year of software maintenance and support will be included under the warranty at no additional cost and begins following the acceptance of the RMS by an Authorized User. No software maintenance or support fees shall be charged to the Authorized User during the warranty period. Subsequent years following the warranty period will be billed by the Contractor on an annual basis at the applicable rate for software maintenance and support specified in Attachment A, Pricing Pages.

7.7 Pricing Structure and Modification.

Contractor must furnish all quantities actually ordered by Authorized Users at or below the prices in Attachment A, Pricing Pages.

Contractor shall provide the Products initially awarded in this Aggregate Agreement, for the entire duration of the Aggregate Agreement including any extensions.

7.7.1 Additional Products.

In addition to the Products initially awarded in this Aggregate Agreement, during the term of the Aggregate Agreement, the Contractor may choose to offer Additional Products. Additional Products are defined as desirable Products that are available

on Contract PM67350. The decision to procure Additional Products will be at the Authorized User's discretion. In order for Additional Products to be added under the Aggregate Agreement, Products must first be approved on the Manufacturer Umbrella Contract in accordance with Contract PM67350, Appendix C.1, Contract Pricing Modification form, as applicable. During the term of the Aggregate Agreement, if Additional Products become available on Contract PM67350, the Contractor may request to add the items to this Aggregate Agreement using the procedure specified in Attachment G, Agreement Modification Procedures.

7.8 Sales Reporting.

The Awarded Contractor shall provide OGS with accurate and timely sales reports containing detailed information of all purchases by state and non-state Authorized Users, political subdivisions and other authorized entities within other State or governmental jurisdictions, made pursuant to this Aggregate Agreement. Sales Reports for this Aggregate Agreement must be submitted to OGS utilizing the format in Attachment F, Sales Report Form and must be submitted separately from the sales reports regularly submitted under the Manufacturer Umbrella Contract.

Sales reports are due one month following the end of each quarter. The quarters for each sales report submission are as follows: January - March; April - June; July - September; October - December.

SECTION 8. RESERVED RIGHTS.

OGS reserves the right to:

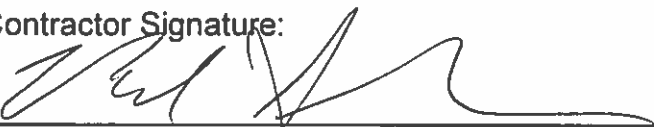
Upon notice to the Contractor, unilaterally incorporate the terms and conditions of any subsequent amendment to the Contract PM67350, including any appendices thereto, into this Aggregate Agreement.

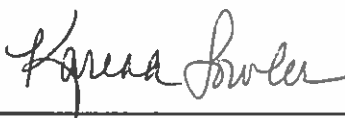
SECTION 9. DISPUTE RESOLUTION PROCESS

Disputes between the Contractor and OGS regarding the Aggregate Agreement will be handled pursuant to sections 64(II)(A) and 64(II)(B) of Appendix B to Contract PM67350. Informal disputes between other Authorized Users and the Contractor will be handled under Appendix B section 64(II)(A), and formal disputes between other Authorized Users and Contractor shall be handled under the Authorized User's dispute procedures.

Signature Page

The undersigned certifies: that s/he is authorized to bind the Contractor referenced below, that the Contractor accepts and acknowledges the award of Request for Quote 18-02, Law Enforcement Records Management System, and that the Contractor agrees to the terms and conditions of this Aggregate Agreement.

Contract # PM67350	Contractor Name Niche Technology Inc.
Contractor Signature: 	Date: December 10, 2018
Printed or Typed Name: Roland Schneider	Title: Secretary/Treasurer
Phone Number: 204 786 2400 x201	Email: Roland.Schneider@NicheRMS.com

The People of the State of New York	
Signature: 	Date: December 11, 2018
Printed or Typed Name: Karen A. Fowler	Title: Director