

NOTICE OF CONTRACT NO. 271B6600001
Between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
BS&A Software 14965 Abbey Lane Bath, MI 48808	Tom Szur	tszur@bsasoftware.com
	TELEPHONE	VENDOR TAX ID # (LAST FOUR DIGITS ONLY)
	517-641-8900	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER:	Treasury	Kevin VanGieson	517-241-4338	vangiesonk@michigan.gov
CONTRACT ADMINISTRATOR:	Treasury	Greg Pawlak	517-636-6819	PawlakG@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: State Assessed Property Data Collection Reporting Services.			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 Year	10/1/2015	9/30/2018	2, one year
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
N/A	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			EXTENDED PURCHASING:
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
N/A			
MISCELLANEOUS INFORMATION:			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:		\$312,000.00	

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation #027115B0004641. Orders for delivery will be issued directly by the Department of Treasury through the issuance of a Purchase Order Form.

Notice of Contract #: 271B660001

FOR THE CONTRACTOR:	FOR THE STATE:
BS&A Software. Firm Name	 Signature
 Authorized Agent Signature	Greg Pawlak Name/Title
Tom Szur Authorized Agent (Print or Type)	Michigan Department of Treasury Enter Name of Agency
09-02-2015 Date	9/3/15 Date

Contract number 271B660001

2

STATE OF MICHIGAN

STANDARD CONTRACT TERMS

271B660001

This STANDARD CONTRACT (“**Contract**”) is agreed to between the State of Michigan (the “**State**”) and BS&A Software (“**Contractor**”), a Michigan company. **This Contract is effective on October 1, 2015 (“Effective Date”), and unless terminated, expires on September 30, 2018.**

The above section will be updated prior to Contract Execution. This Contract term will be for a period of three (3) years.

This Contract may be renewed for up to two additional one-year period(s). Renewal must be by written agreement of the parties.

The parties agree as follows:

1. **Duties of Contractor.** Contractor must perform the services and provide the deliverables described in **Exhibit A – Statement of Work** (the “**Contract Activities**”). An obligation to provide delivery of any commodity is considered a service and is a Contract Activity.

Contractor must furnish all labor, equipment, materials, and supplies necessary for the performance of the Contract Activities, and meet operational standards, unless otherwise specified in Exhibit A.

Contractor must: (a) perform the Contract Activities in a timely, professional, safe, and workmanlike manner consistent with standards in the trade, profession, or industry; (b) meet or exceed the performance and operational standards, and specifications of the Contract; (c) provide all Contract Activities in good quality, with no material defects; (d) not interfere with the State’s operations; (e) obtain and maintain all necessary licenses, permits or other authorizations necessary for the performance of the Contract; (f) cooperate with the State, including the State’s quality assurance personnel, and any third party to achieve the objectives of the Contract; (g) return to the State any State-furnished equipment or other resources in the same condition as when provided when no longer required for the Contract; (h) not make any media releases without prior written authorization from the State; (i) assign to the State any claims resulting from state or federal antitrust violations to the extent that those violations concern materials or services supplied by third parties toward fulfillment of the Contract; (j) comply with all State physical and IT security policies and standards which will be made available upon request; and (k) provide the State priority in performance of the Contract except as mandated by federal disaster response requirements. Any breach under this paragraph is considered a material breach.

Contractor must also be clearly identifiable while on State property by wearing identification issued by the State, and clearly identify themselves whenever making contact with the State.

2. **Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

<p>If to State:</p> <p><i>Greg Pawlak</i> <i>7285 Parsons Drive</i> <i>Dimondale, MI 48821</i> PawlakG@michigan.gov <i>517-636-6819</i></p>	<p>If to Contractor:</p> <p><i>Tom Szur</i> <i>14965 Abbey Lane</i> <i>Bath, MI 48808</i> tszur@bsasoftware.com <i>517-641-8900</i></p>
---	--

3. **Contract Administrator.** The Contract Administrator for each party is the only person authorized to modify any terms and conditions of this Contract (each a “**Contract Administrator**”):

<p>If to State: <i>Greg Pawlak</i> 7285 Parsons Drive Dimondale, MI 48821 PawlakG@michigan.gov 517-636-6819</p>
--

4. **Program Manager.** The Program Manager for each party will monitor and coordinate the day-to-day activities of the Contract (each a “**Program Manager**”):

<p>State: <i>Kevin VanGieson</i> 430 West Allegan Lansing, MI, 48922 [Email] vangiesonk@michigan.gov [Phone] 517-241-4338</p>

5. **Performance Guarantee.** Contractor must at all times have financial resources sufficient, in the opinion of the State, to ensure performance of the Contract and must provide proof upon request. The State may require a performance bond (as specified in Exhibit A) if, in the opinion of the State, it will ensure performance of the Contract.

6. **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A" or better and a financial size of VII or better.

Insurance Type	Additional Requirements
Commercial General Liability Insurance	
<p><u>Minimal Limits:</u> \$1,000,000 Each Occurrence Limit \$1,000,000 Personal & Advertising Injury Limit \$2,000,000 General Aggregate Limit \$2,000,000 Products/Completed Operations</p> <p><u>Deductible Maximum:</u> \$50,000 Each Occurrence</p>	<p>Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 0.</p>
Umbrella or Excess Liability Insurance	
<p><u>Minimal Limits:</u> \$5,000,000 General Aggregate</p>	<p>Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds.</p>

Automobile Liability Insurance	
<u>Minimal Limits:</u> \$1,000,000 Per Occurrence	
Workers' Compensation Insurance	
<u>Minimal Limits:</u> Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
<u>Minimal Limits:</u> \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
<u>Minimal Limits:</u> \$1,000,000 Each Occurrence \$2,000,000 Annual Aggregate	Contractor must have their policy: (1) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

Professional Liability (Errors and Omissions) Insurance	
<u>Minimal Limits:</u> \$1,000,000 Each Occurrence \$2,000,000 Annual Aggregate <u>Deductible Maximum:</u> \$50,000 Per Loss	
Property Insurance	
Property Insurance covering any loss or damage to the State-owned office space used by Contractor for any reason under this Contract, and the State-owned equipment, software and other contents of the office space, including without limitation, those contents used by Contractor to provide the Services to the State, up to its replacement value, where the office space and its contents are under the care, custody and control of Contractor. The State must be endorsed on the policy as a loss payee as its interests appear.	

If any of the required policies provide **claim-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

This Section is not intended to and is not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

7. RESERVED

8. RESERVED

9. Independent Contractor. Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. The Contractor hereby acknowledges that the State is and will be the sole and exclusive owner of all right, title, and interest in the Contract Activities and all associated intellectual property rights, if any. Such Contract Activities are works made for hire as defined in Section 101 of the Copyright Act of 1976. To the extent any Contract Activities and related intellectual property do not qualify as works made for hire under the Copyright Act, Contractor will, and hereby does, immediately on its creation, assign, transfer and otherwise convey to the State, irrevocably and in perpetuity, throughout the universe, all right, title and interest in and to the Contract Activities, including all intellectual property rights therein.

10. Subcontracting. Contractor may not delegate any of its obligations under the Contract without the prior written approval of the State. Contractor must notify the State at least 90 calendar days before the proposed delegation, and provide the State any information it requests to determine whether the

delegation is in its best interest. If approved, Contractor must: (a) be the sole point of contact regarding all contractual matters, including payment and charges for all Contract Activities; (b) make all payments to the subcontractor; and (c) incorporate the terms and conditions contained in this Contract in any subcontract with a subcontractor. Contractor remains responsible for the completion of the Contract Activities, compliance with the terms of this Contract, and the acts and omissions of the subcontractor. The State, in its sole discretion, may require the replacement of any subcontractor.

11. **Staffing.** The State's Contract Administrator may require Contractor to remove or reassign personnel by providing a notice to Contractor.
12. **Background Checks.** Upon request, Contractor must perform background checks on all employees and subcontractors and its employees prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks.
13. **Assignment.** Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation, provide all necessary documentation and signatures, and continue to perform, with the third party, its obligations under the Contract.
14. **Change of Control.** Contractor will notify, at least 90 calendar days before the effective date, the State of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following: (a) a sale of more than 50% of Contractor's stock; (b) a sale of substantially all of Contractor's assets; (c) a change in a majority of Contractor's board members; (d) consummation of a merger or consolidation of Contractor with any other entity; (e) a change in ownership through a transaction or series of transactions; (f) or the board (or the stockholders) approves a plan of complete liquidation. A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes.

In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

15. **Ordering.** Contractor is not authorized to begin performance until receipt of authorization as identified in Exhibit A.
16. **Acceptance.** Contract Activities are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("**State Review Period**"), unless otherwise provided in Exhibit A. If the Contract Activities are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Contract Activities are accepted, but noted deficiencies must be corrected; or (b) the Contract Activities are rejected. If the State finds material deficiencies, it may: (i) reject the Contract Activities without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with Section 23, Termination for Cause.

Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Contract Activities, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Contract Activities to the State. If acceptance with deficiencies or rejection of the Contract Activities impacts the content or delivery of other non-completed Contract Activities, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may perform the Contract Activities and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

17. **RESERVED.**
18. **Risk of Loss and Title.** Until final acceptance, title and risk of loss or damage to Contract Activities remains with Contractor. Contractor is responsible for filing, processing, and collecting all damage claims. The State will record and report to Contractor any evidence of visible damage. If the State rejects the

Contract Activities, Contractor must remove them from the premises within 10 calendar days after notification of rejection. The risk of loss of rejected or non-conforming Contract Activities remains with Contractor. Rejected Contract Activities not removed by Contractor within 10 calendar days will be deemed abandoned by Contractor, and the State will have the right to dispose of it as its own property. Contractor must reimburse the State for costs and expenses incurred in storing or effecting removal or disposition of rejected Contract Activities.

19. Warranty Period. The warranty period, if applicable, for Contract Activities is a fixed period commencing on the date specified in Exhibit A. If the Contract Activities do not function as warranted during the warranty period the State may return such non-conforming Contract Activities to the Contractor for a full refund.

20. Terms of Payment. Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in Exhibit A. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the State's exclusive use. Notwithstanding the foregoing, all prices are inclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Contract Activities. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/cpexpress> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

21. Liquidated Damages. Liquidated damages, if applicable, will be assessed as described in Exhibit A.

22. Stop Work Order. The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate the Contract or purchase order. The State will not pay for Contract Activities, Contractor's lost profits, or any additional compensation during a stop work period.

23. Termination for Cause. The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (a) endangers the value, integrity, or security of any location, data, or personnel; (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; (c) engages in any conduct that may expose the State to liability; (d) breaches any of its material duties or obligations; or (e) fails to cure a breach within the time stated in a notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

If the State terminates this Contract under this Section, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of the Contract, the termination will be deemed to have been a Termination for Convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in Section 24, Termination for Convenience.

The State will only pay for amounts due to Contractor for Contract Activities accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Contract Activities from other sources.

24. Termination for Convenience. The State may immediately terminate this Contract in whole or in part without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance of the Contract Activities immediately, or (b) continue to perform the Contract Activities in accordance with Section 25, Transition Responsibilities. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities.

25. Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract Activities to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Contract Activities to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Contract Activities at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Contract Activities, training, equipment, software, leases, reports and other documentation, to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed deliverables prepared under this Contract as of the Contract termination date; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

26. General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any intellectual property right or other right of any third party; (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations.

The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel; and to (iv) retain control of the defense if the State deems necessary. Contractor will not, without the State's written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27. Infringement Remedies. If, in either party's opinion, any piece of equipment, software, commodity, or service supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the equipment, software, commodity, or service, or if this option is not reasonably available to Contractor, (b) replace or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

28. Limitation of Liability. The State is not liable for consequential, incidental, indirect, or special damages, regardless of the nature of the action.

29. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a subcontractor, or an officer or director of Contractor or subcontractor, that arises during the term of the Contract, including: (a) a criminal Proceeding; (b) a parole or probation Proceeding; (c) a Proceeding under the Sarbanes-Oxley Act; (d) a civil Proceeding involving: (1) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or (2) a governmental or public entity's claim or written allegation of fraud; or (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

30. State Data.

- a. Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes: (a) the State's data collected, used, processed, stored, or generated as the result of the Contract Activities; (b) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Contract Activities, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and, (c) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Contract Activities, which is defined under the Health Insurance Portability and Accountability Act (HIPAA) and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This Section survives the termination of this Contract.
- b. Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Contract Activities, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Contract Activities. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Contract Activities, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This Section survives the termination of this Contract.
- c. Extraction of State Data. Contractor must, within five (5) business days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of the State Data in the format specified by the State.
- d. Backup and Recovery of State Data. Unless otherwise specified in Exhibit A, Contractor is responsible for maintaining a backup of State Data and for an orderly and timely recovery of such data. Unless otherwise described in Exhibit A, Contractor must maintain a contemporaneous backup of State Data that can be recovered within two (2) hours at any point in time.
- e. Loss of Data. In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less

than twenty-four (24) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (g) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and, (h) provide to the State a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. This Section survives the termination of this Contract.

31. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. The provisions of this Section survive the termination of this Contract.

- a. Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.
- b. Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this Section.
- c. Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.
- d. Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing

undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

- e. Surrender of Confidential Information upon Termination. Upon termination of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control; provided, however, that Contractor must return State Data to the State following the timeframe and procedure described further in this Contract. Should Contractor or the State determine that the return of any non-State Data Confidential Information is not feasible, such party must destroy the non-State Data Confidential Information and must certify the same in writing within 5 calendar days from the date of termination to the other party.

32. Data Privacy and Information Security.

- a. Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all employees, agents, and subcontractors of Contractor, if any, comply with all of the foregoing. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable State IT policies and standards, which are available to Contractor upon request.
- b. Audit by Contractor. No less than annually, Contractor must conduct a comprehensive independent third-party audit of its data privacy and information security program and provide such audit findings to the State.
- c. Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Contract Activities and from time to time during the term of this Contract. During the providing of the Contract Activities, on an ongoing basis from time to time and without notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within 45 calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.
- d. Audit Findings. Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.
- e. State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this Section.

33. RESERVED

34. RESERVED

- 35. Records Maintenance, Inspection, Examination, and Audit.** The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to the Contract through the term of the Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Audit Period, Contractor must retain the records until all issues are resolved.

Within 10 calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Contract Activities are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If any financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of the Contract must be paid or refunded within 45 calendar days.

This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

- 36. Warranties and Representations.** Contractor represents and warrants: (a) Contractor is the owner or licensee of any Contract Activities that it licenses, sells, or develops and Contractor has the rights necessary to convey title, ownership rights, or licensed use; (b) all Contract Activities are delivered free from any security interest, lien, or encumbrance and will continue in that respect; (c) the Contract Activities will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (d) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (e) the Contract Activities are merchantable and fit for the specific purposes identified in the Contract; (f) the Contract signatory has the authority to enter into this Contract; (g) all information furnished by Contractor in connection with the Contract fairly and accurately represents Contractor's business, properties, finances, and operations as of the dates covered by the information, and Contractor will inform the State of any material adverse changes; and (h) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading. A breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under Section 23, Termination for Cause.
- 37. Conflicts and Ethics.** Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.
- 38. Compliance with Laws.** Contractor must comply with all federal, state and local laws, rules and regulations.
- 39. RESERVED**
- 40. Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, or mental or physical disability. Breach of this covenant is a material breach of this Contract.
- 41. Unfair Labor Practice.** Under MCL 423.324, the State may void any Contract with a Contractor or subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.
- 42. Governing Law.** This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.
- 43. Non-Exclusivity.** Nothing contained in this Contract is intended nor will be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Contract Activities from other sources.
- 44. Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of god that are beyond their control and without their fault or negligence. Each party will

use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.

- 45. Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely, or fails to respond within 15 business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

- 46. Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.

- 47. Website Incorporation.** The State is not bound by any content on Contractor's website unless expressly incorporated directly into this Contract.

- 48. Order of Precedence.** In the event of a conflict between the terms and conditions of the Contract, the exhibits, a purchase order, or an amendment, the order of precedence is: (a) the purchase order; (b) the amendment; (c) Exhibit A; (d) any other exhibits; and (e) the Contract.

- 49. Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

- 50. Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.

- 51. Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.

- 52. Entire Contract and Modification.** This Contract is the entire agreement and replaces all previous agreements between the parties for the Contract Activities. This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**").

EXHIBIT A



STATEMENT OF WORK State Assessed Property Tax Collection Services

1.1 PURPOSE AND BACKGROUND

This is a Contract for State Assessed Property Data Collection and Reporting Services in an electronic format acceptable for use with the State Assessed Property process for the Michigan Department of Treasury. The Data Collection and Reporting Services include compilation, input, output, and analysis of assessment data currently submitted via State Tax Commission Forms 1027, 1028, 1029, and applicable tax credit applications from State Assessed entities. State Assessed entities include telephone, railroad, and railcar companies that own, lease, operate, or use lines in Michigan. State Assessed property reporting is mandated by Michigan Public Act 282 of 1905, as amended.

The State Assessed Property assessment system is the basis for the collection of approximately 50 million dollars in property taxes annually. Currently, most information is supplied to the Assessment and Certification Division (ACD) by State Assessed reporting entities or their tax representatives on web based forms. Reports are produced to provide required rolls, notices, and tax bills.

This Contract will be effective October 1, 2015, through September 30, 2018.

1.2 REQUIREMENTS

The Contractor must develop an electronic system to collect, store and create report assessment data currently provided on Forms 1027, 1028, 1029, and applicable tax credit applications for each reporting year that would also include prior year information. The Contractor must allow the entry of estimated assessment information into the system on behalf of a small percentage of reporting entities that fail or refuse to make annual reports as needed.

The Contractor must provide annual reports in paper and CD formats from Forms 1027, 1028, 1029, and applicable tax credit applications to meet requirements of Treasury retention schedules.

A. Electronic Web-based System General Requirements:

A.1. The Contractor's Web-based system must permit state assessed entities to enter asset-cost data, asset and taxpayer descriptive data, and tax credit application data, as determined by the ACD, in an electronic format to a secure online account which can be accessed with a unique personal identification number (PIN).

A.2. The Contractor's Web-based system must permit correction and maintenance of report data by ACD staff between the First day of January and mid-June, for the creation of tentative and final assessment rolls, notices, and tax bills.

A.3. The Contractors Web-based system must electronically calculate the following values in accordance with valuation methodologies established by the ACD:

- a. Tentative True Cash Value
- b. Tentative Assessed Value
- c. Tentative Capped Value
- d. Tentative Taxable Value

- A.4. The Contractors Web-based system must permit the production of tentative assessment reports as approved and prescribed by ACD and a tentative state assessed roll for submission at the May STC Meeting for Tentative State Assessed Roll each year, beginning in **May of 2016**. The tentative state assessed roll shall be in the same general format as is currently used and shall include for each state assessed entity:
- a. The name of the taxpayer
 - b. The mailing address of the taxpayer
 - c. The parcel identification number for the taxpayer
 - d. The tentative True Cash Value for the taxpayer
 - e. The tentative Assessed Value for the taxpayer
 - f. The tentative Capped Value for the taxpayer
 - g. The tentative Taxable Value for the taxpayer
 - h. Any other data content directed by the ACD
- A.5. The Contractors Web-based system must provide electronically formatted Tentative Assessment Notices as approved and prescribed by ACD for mailing to each taxpayer that will permit ACD to produce assessment notices in the same general format as is currently used. The assessment notices produced shall be formatted for insertion in Treasury window envelopes. The notices shall be provided the day after the tentative state assessed roll is approved by the STC. Each assessment notice shall include the information contained on the tentative assessment roll as it relates to each particular taxpayer.
- A.6. The Contractors Web-based system must prepare a summary of change report which summarizes all of the changes from the tentative assessment roll to the final assessment roll.
- A.7. The Contractors Web-based system must permit the production of final assessment reports as approved and prescribed by ACD and a final state assessed roll for submission at the **June STC Meeting for Final State Assessed Roll each year. Beginning June of 2016**, the final state assessed roll shall be in the same general format as is currently used and shall include for each taxpayer:
- a. The name of the taxpayer
 - b. The mailing address of the taxpayer
 - c. The parcel identification number for the taxpayer
 - d. The final True Cash Value for the taxpayer
 - e. The final Assessed Value for the taxpayer
 - f. The final Capped Value for the taxpayer
 - g. The final Taxable Value for the taxpayer
 - h. Any other data content directed by the ACD
- A.8. The Contractors Web-based system must permit the production of assessment tax roll reports as approved and prescribed by ACD and the creation of tax bills containing the following for each taxpayer:
- a. Name of the taxpayer
 - b. Address of the taxpayer
 - c. Parcel identification number for the taxpayer
 - d. True Cash Value
 - e. Final Assessed Value
 - f. Final Capped Value
 - g. Final Taxable Value
 - h. Gross Tax Due
 - i. Any Applicable Tax Credits
 - j. Net Tax Due
 - k. Any other data content directed by the ACD
- A.9. The Contractors Web-based system must permit ACD to obtain data and reports from the online system to make necessary changes during review and throughout the year. To accomplish this, the Contractor shall develop and maintain the system and provide necessary deliverables in a manner such that:

1. A limited number of ACD staff, identified by the Program Manager must have read and write access to data and reports.
 2. State Assessed reporting entities must have write access for initial submission of data and read-only access to data after initial submission.
 3. ACD staff has the ability to make assessment roll and tax billing changes at any time for MCL 211.154, Michigan Tax Tribunal, etc. actions as they may occur.
 4. ACD staff has the ability to make taxpayer address correction/changes as needed throughout the year.
 5. Contractor will also load updated assessment information to one ACD laptop computer after creation of the tentative and final assessment rolls.
- A.10. The Contractors Web-based system must provide 99% availability 24 hours per day, seven days per week and further:
- a. The Contractor must notify the Program Manager 24 hours prior to any scheduled down time.
- A.11. The Contractors Web-based system must have the ability to accommodate future changes such as changes in the number or type of reporting entities and changes in statutes or reporting requirements. Changes must be requested in writing by the State of Michigan Program Manager and must be charged at the per hour rate identified in the pricing page.
- A.12. The Contractors Web-based system shall require identification of individual users and authentication of data submitted on behalf of the reporting entity and further:
- a. The system must allow only one user per reporting entity to submit and view data.
 - b. The system must include control mechanisms in place to maintain integrity of data during transmission and storage.
- A.13. The Contractors Web-based system must retain data and reports for a minimum of seven years. The State Program Manager will be notified in writing, before any data is to be removed from the Reporting and Assessment System.
- A.14. The Contractors Web-based system must provide all data and reports via a web browser, Microsoft Internet Explorer version 9.0 or later. There must be no additional software or hardware required to access the data and reports.
- A.15. The Contractors Web-based system must have a response time with minimal delay for the end-user. "Minimal delay" is to be defined as meeting the following requirement: Data must populate within 10 seconds, and reports must populate within one minute.
- A.16. The Contractors Web-based system must provide telephone support from 8:00 a.m. to 5:00 p.m. Eastern Standard Time (EST) Monday through Friday (excluding observed State Holidays) and must respond to concerns within two business days.
- A.17. The Contractors Web-based system must ensure any modifications to the reporting system are transparent to users and not require any updates on computers.
- A.18. The Contractors Web-based system must provide all data entry, maintenance, back-up and recovery of the web-based system.
- A.19. The Contractor Web-based system must provide all system upgrades to ACD Staff, at no additional cost, during the term of the Contract.
- A.20. The Contractors Web-based system must back up the data a minimum of one time per week (daily update preferred).
- A.21. The Contractors Web-based system must provide a disaster recovery and business continuity plan.

- A.22. The Contractor must notify the State Program Manager 24 hours in advance of any scheduled downtime. All system outages/shutdowns must be reported immediately to the Program Manager or State's designee. Within 24 hours of problem resolution and restart, the Contractor must prepare and submit a report to the Program Manager or State's designee indicating elapsed downtime hours, start/end timeframes, reason for the outage, impact on the systems (lost data, etc.) for each occurrence and resolution to mitigate future occurrences.
- A.23. The Contractor must provide quality assurance measures for entire process to ensure data integrity, accuracy, and consistency.
- A.24. The Contractor should monitor and be able to provide Program Manager with suggestions of enhancements or efficiencies for entire process as discovered.
- A.25. The Contractor must comply with the State of Michigan Security Requirements. See Exhibit 1.
- A.26. The Contractor must comply with the Exhibit 2 Safeguard Requirements of Confidential Data.

B. General Process Requirements:

- B.1. The Contractor must create a Tentative State Assessed Roll and Notices based on assessment information
- B.2. The Contractor must create a Final State Assessed Roll and Notices based on assessment information
- B.3. The Contractor must create a Final State Assessed Tax Roll and Tax Bills based on assessment information
- B.4. The developed reports for each process must:
- Contain the same data fields and format as current annual reports approved by the State Tax Commission each year on Forms 1027, 1028, 1029, and applicable tax credit applications.
 - Have the ability to be printed to letter size paper using Adobe Acrobat 6.0 or higher.
 - Be formatted to enable printing of the entire annual report including real property lists and values for telephone companies.
 - Show valuation totals of calculations of true cash values for each report table and total of all tables on each report.
 - Telephone annual reports will also allow the ability to report real property changes and valuation changes for any parcel.

C. FORM 4435 PIN and Parcel Numbering Process Requirements:

- C.1. The Contractor must:
- Create and provide ACD staff with a unique six digit personal identification number (PIN) for each state assessed parcel (both current and new reporting parcels) before the First of January each year. This PIN, when combined with the assigned state assessed parcel number, will allow a reporting entity to enter the secured website for both reporting and viewing of assessment information. The confidential PIN information will be sent by ACD staff to all requesting entities on Form 4435.
 - Follow the current established parcel numbering system:
 - 97-00-00-00-000-XXX for railcar companies
 - 98-00-00-00-000-XXX for railroad companies
 - 99-00-00-00-000-XXX for telephone companies
 - Retain the same numbering system established for telephone real property locations. Those parcels are numbered by using information specific to each real property location
 - Provide ACD staff with special access PINs for the ability to review and make corrections to any annual reports.

D. FORM 1027 Process Requirements for Railcar Reporting:

- D.1. The Contractor must:
- Receive and process Form 1027 in an electronic format from the reporting entity.

- b. Receive and process tax credit application if applicable.
- c. Allow for the reporting of multiple railcar marks within an individual reporting parcel.
- d. Allow for ACD staff entry of estimated assessment information into the system on behalf of reporting entities that fail or refuse to make annual reports as needed.
- e. There were approximately 350 reporting railcar parcels for 2014.

E. FORM 1028 Process Requirements for Railroad Reporting:

E.1. The Contractor must:

- a. Receive and process Form 1028 in an electronic format from the reporting entity.
- b. Receive and process tax credit application if applicable.
- c. Allow for the weighted calculation of cost and income approaches to value.
- d. Allow for ACD staff entry of estimated assessment information into the system on behalf of reporting entities that fail or refuse to make annual reports as needed.
- e. There were approximately 30 reporting railroad parcels for 2014.

F. FORM 1029 Process Requirements for Telephone Reporting:

F.1. The Contractor must:

- a. Receive and process Form 1029 in an electronic format from the reporting entity.
- b. Receive and process tax credit applications if applicable.
- c. Allow for reporting of changes to real property locations (both new and existing locations).
- d. Allow for the combination of both real and personal property as one assessment for each company with real property locations.
- e. Allow for ACD staff entry of estimated assessment information into the system on behalf of reporting entities that fail or refuse to make annual reports as needed.

Note: There were approximately 100 reporting telephone companies for 2014 with approximately 1,535 real property locations for 2014.

1.3 ACCEPTANCE

1.3.1 Final Acceptance

Final Acceptance is when final review of all deliverables is completed and accepted by the State per Exhibit A, and all requirements of the Contract are met.

1.4 STAFFING

1.4.1 Contractor Representative

The Contractor appointed Account Representative, specifically assigned to State of Michigan accounts that will be **Tom Szur**. Tom must respond to State inquiries regarding the Contract Activities, answering questions related to ordering and delivery, etc. (the "Contractor Representative").

The Contractor must notify the Contract Administrator at least 30 calendar days before removing or assigning a new Contractor Representative.

1.4.2 Technical Support, Repairs and Maintenance

The Contractors phone number for the State to make contact with the Contractor for technical support, repairs and maintenance is (517) 641-8900 and toll free at (855) BSA-SOFT. The Contractor must be available for calls and service during the hours of 8 am to 5 pm EST

1.4.3 Work Hours

1.4.4 The Contractor must provide Contract Activities during the State’s normal working hours Monday – Friday 8:00 a.m. to 5:00 p.m. EST, and possible night and weekend hours depending on the requirements of the project.

1.4.5 Key Personnel

1. The Contractor must:
 - a. Carry out this project under the direction and control of the **Program Manager Tom Szur**.
 - b. The Contractors Project Manager for this contract is **Scott Gross (CMAE-3)**. Scott shall act as a central point of contact for all Contractual activities.
 - c. The Contractor’s Project Manager must meet with the State Program Manager monthly, at a minimum, or as requested by the states Program Manager for the purpose of reviewing progress and providing necessary guidance to the Contractor in solving problems which arise, although there will be continuous liaison with the Contractor team.
 - d. The Contractor must attend State meetings and conference calls with Treasury personnel as needed and determined by the Program Manager. The Contractor must respond to phone calls and email requests from Program Manager within one business day.
 - e. The Contractor’s full and part time staff must possess a sufficient understanding of State Assessed property and State Tax Commission procedures. **The Contractor must employ one or more project review managers, certified as Michigan Master Assessing Officer (Level 4) or Michigan Advanced Assessing Officer (Level 3) to ensure accuracy, quality, and consistency of state assessed property.**
 - f. The contractor must have sufficient qualified staff to properly complete the assessment process. The Contractor must identify below the number of certified assessors by name and level in its employment.

EMPLOYEE NAME	LEVEL	ROLE
Scott Gross	3 (MAAO)	Assessing Support Director, Project Manager for this RFP
Dan Bengel	3 (MAAO)	Assessing Support
Tom Schafer	3 (MAAO)	Assessing Support
Jason Kohagen	3 (MAAO)	Assessing Support
Kelly Garner	3 (MAAO)	Implementation & Training Services

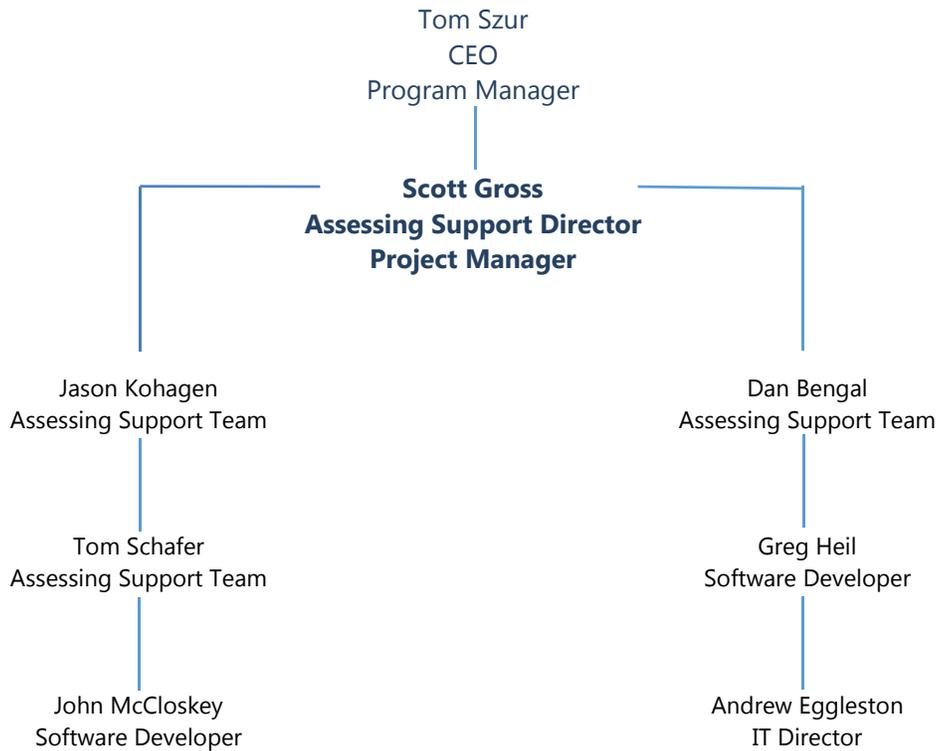
- g. The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State’s Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection. The State may require a 30-calendar day training period for replacement personnel.
- h. The Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor’s removal of Key Personnel without the prior written consent of the State is an unauthorized removal (“**Unauthorized Removal**”). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel’s employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under Termination for Cause in the Standard Terms.
 - (i) For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the credit amount will be \$25,000.00 per individual if Contractor identifies a replacement approved by

the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30 calendar days before the Key Personnel's removal.

- (ii) If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 calendar days, in addition to the \$25,000.00 credit specified above, Contractor will credit the State \$833.33 per calendar day for each day of the 30 calendar-day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30 calendar days of shadowing will not exceed \$50,000.00 per individual.

1.4.6 Organizational Chart

The Contractor overall organizational chart that details staff members, by name and title, and subcontractors. See organizational chart attachment.



1.4.7 Disclosure of Subcontractors

There are no Subcontractors currently being used by the Contractor to perform the work described in Exhibit A. If the Contractor intends to utilize subcontractors at a later date, the Contractor must disclose the their intent to use a Subcontractor and the State must approve in writing.

1.4.8 Security

The Contractor will be subject to the Safeguard Requirements of Confidential Data (Exhibit A)
Bidder Response:

The Contractors staff may be required to make deliveries to or enter State facilities. The bidder must: (a) explain how it intends to ensure the security of State facilities, (b) whether it uses uniforms and ID badges, etc., (c) identify the company that will perform background checks, and (d) the scope of the background checks. The State may require the Contractor's personnel to wear State issued identification badges.

1.5 PROJECT MANAGEMENT

1.5.1 Project Plan

1. Within five working days of the Contract start date, the Contractor must submit a project plan to the State Program Manager for final approval.

1.5.2 Reporting

The Contractor must submit brief written monthly summaries of progress which outline the work accomplished during the reporting period; work to be accomplished during the subsequent reporting period; problems, real or anticipated, which must be brought to the attention of the client Agency's Project Director; and notification of any significant deviation from previously agreed-upon work plans.

1.6 ORDERING

1.6.1 Authorizing Document

The appropriate authorizing document for the Contract will be Purchase Order of an agreed upon Blanket Purchase Order.

1.7 INVOICE AND PAYMENT

1.7.1 Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order; (c) quantity; (d) description of the Contract Activities; (e) unit price; (f) shipping cost (if any); and (g) total price. Overtime, holiday pay, and travel expenses will not be paid.

1.8 Liquidated Damages

Late or improper completion of the Contract Activities will cause loss and damage to the State and it would be impracticable and extremely difficult to fix the actual damage sustained by the State. Therefore, if there is late or improper completion of the Contract Activities the State is entitled to collect liquidated damages in the amount of \$5,000 and an additional \$100 per day for each day Contractor fails to remedy the late or improper completion of the Work.

EXHIBIT B - RESERVED



EXHIBIT C



PRICING

A. The Contractors firm pricing schedule for the Contract Activities.

State of Michigan – State Assessed Property Taxes – Years 2015 - 2017

State of Michigan – State Assessed Property Taxes: Years 2015- 2017

Compile Tentative Assessment Roll	\$ 30,000
--	------------------

The Contractor will complete all tasks necessary to assemble the Tentative Assessment Roll. The Contractor will employ all standard mass appraisal techniques.

Compile Final Assessment Roll	\$ 13,000
--------------------------------------	------------------

The Contractor must complete all tasks necessary to assemble the Final Assessment Roll.

Import data from State assessed company annual reports and other state resources.	\$ 9,000
--	-----------------

The listed fee is for the data entry and Valuation of the newly assessed real property parcels each year.

Process Personal Property reports submitted by State assessed companies, Incorporating the State Tax Commission Tables	\$14,000
---	-----------------

Note – Data entry on the e-Filed Personal Property Form for this project will be completed by either the Taxpayer (self-reporting), or Treasury Staff (paper file).

The Contractor will electronically process each personal property form within the Equalizer Assessing System after it is 'validated' by Treasury staff. The fee for this service includes the management of the process and verification of data submitted into the underlying database. The Contractor is responsible for the final value placed on the Assessment Roll and the Tax Roll after submission. The Contractor will run various Data integrity checks to assure data is accurate.

Cost to develop Internet-based reporting system for State assessed properties one time setup fee (web interface for e-filing Personal Property Statements:	\$ 0
---	-------------

Annual Maintenance Fee:

\$ 8,000

Annual service fee for the updating and maintenance of the web forms/infrastructure and underlying program and forms specific to the e-Personal Property project of State Assessed Properties. Maintenance invoicing shall be ½ payment in March/April and ½ July equaling an annual maintenance fee of \$8000.00.

Assemble and Compile Tax Roll

Create Tax Bills – one summary for each company

\$ 6,000

- a) Compile Tax Roll
- b) Prepare Original Roll
- c) Calculate Bills
- d) Balance to 'warrants' or other State Documents
- e) Create PDFs of Tax Bills
- f) Deliver completed bills to state
- g) Deliver Reports to State

Adjust for additional 1% per month interest on late payments; and other adjustments to balance tax rolls

\$ 2,000

Internet Service Fee – posting data on the Web

\$ 5,000

Meeting/Phone Calls/Emails/Correspondence

\$ 2,000

Custom programming/imports/exports/reports

\$15,000

- a) Tax Administration Application – \$3,000
- b) Assessing Application - \$4,000
- c) Internet/Web Display App – \$3,000
- d) e-Personal Property Web Forms – \$5,000

Option Year Pricing:

4th Year

\$104,000

5th Year

\$104,000

First-Year Contract Total:	\$ 104,000
Firm Year Two and Three Pricing (104,000 x 2):	\$ 208,000
3 Year Contract Total:	<u>\$ 312,000</u>

EXHIBIT 1



SECURITY REQUIREMENTS

On award of the Contract, the Contractor must comply with State and Federal statutory and regulatory requirements, and rules; National Institute of Standards and Technology (NIST) publications; Control Objectives for Information and Related Technology (COBIT); all other industry specific standards; national security best practices and all requirements herein.

The Contractor must perform annual testing of all security control requirements to determine they are working as intended. Annual certification must be provided in writing to the Program Manger/CCI or designee in the form of a SSAE16 or similar audit report, if applicable.

A. Governing Security Standards and Publications

The State of Michigan information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised.

The Contractor must collect, process, store, and transfer Department of Treasury personal, confidential or sensitive data in accordance with the contractual agreement, State of Michigan policies and the laws of the State of Michigan and the United States, including but is not limited to the following:

1. The Michigan Identity Theft Protection Act, MCL 445.61 et seq;
2. The Michigan Social Security Number Privacy Act, MCL 445.82 et seq.
3. Family Educational Rights and Privacy Act
4. State of Michigan Policies: The Contractor must comply with the State of Michigan information technology standards (<http://www.michigan.gov/dmb/0,4568,7-150-56355-108233--,00.html>).

B. Security Risk Assessment

The Contractor must conduct assessments of risks and identify the damage that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department of Treasury. Security controls should be implemented based on the potential risks. The

Contractor must ensure that reassessments occur whenever there are significant modifications to the information system and that risk assessment information is updated.

C. System Security Plan

The Contractor must develop and implement a security plan that provides an overview of the security requirements for the information system. If a security plan does not exist, the contractor shall provide a description of the security controls planned for meeting those requirements. The security plan must be reviewed periodically and revised to address system/organizational changes or problems.

D. Network Security

The Contractor is responsible for the security of and access to Department of Treasury data, consistent with legislative or administrative restrictions. Unsecured operating practices, which expose other connected networks to malicious security violations, are not acceptable. The Contractor must coordinate with the Michigan Department of Technology, Management and Budget to enter the proper pointers into the State of Michigan infrastructure.

E. Data Security

The Contractor has the responsibility to protect the confidentiality, integrity, and availability of State of Michigan data that is generated, accessed, modified, transmitted, stored, disposed, or used by the system, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

The Contractor must:

1. process the personal data in accordance with the personal data protection laws of the State of Michigan and the United States.
2. have in place appropriate technical and organizational internal and security controls to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. Technical and organizational security controls must be implemented that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing.
3. provide secure and acceptable methods of transmitting personal, confidential or sensitive information over telecommunication devices such as data encryption (128 bit minimum), Secure Socket Layer (SSL), dedicated leased line or Virtual Private Network (VPN).
4. supply the Department of Treasury, Security Division with information associated with security audits performed in the last three years.

5. have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality, integrity, and availability of the data.
6. process the personal, confidential and sensitive data only for purposes described in the contract.
7. identify to the Department of Treasury a contact point within its organization authorized to respond to enquiries concerning processing of the personal, confidential or sensitive data, and will cooperate in good faith with the Department.
8. not disclose or transfer the personal, confidential or sensitive data to a third party unless it is approved under this contract.
9. not use data transferred by the Department of Treasury as a result of this contract for marketing purposes.

F. Media Protection

1. The Contractor must implement measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media containing Department of Treasury's personal, confidential and sensitive information to prevent the loss of confidentiality, integrity, or availability of information including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.
2. The Contractor must ensure that only authorized users have access to information in printed form or on digital media removed from the information system, physically control and securely store information media, both paper and digital, restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

G. Media Destruction and Disposal

1. **The Contractor must sanitize or destroy information system digital media containing personal, confidential or sensitive information before its disposal or release for reuse to prevent unauthorized individuals from gaining access to and using information contained on the media.**
2. **Personal, confidential or sensitive information must be destroyed by burning, mulching, pulverizing or shredding. If shredded, strips should not be more than 5/16-inch, microfilm should be shredded to affect a 1/35-inch by 3/8-inch strip, and pulping should reduce material to particles of one inch or smaller.**
3. Disk or tape media must be destroyed by overwriting all data tracks a minimum of three times or running a magnetic strip over and under entire area of disk at least three (3) times. If the CD, DVD or tape cannot be overwritten it must be destroyed in an obvious manner to prevent use in any disk drive unit and discarded. Hand tearing, recycling, or burying

information in a landfill are unacceptable methods of disposal. Electronic data residing on any computer systems must be purged based on retention periods required by the Department of Treasury.

H. Access Control

The Contractor must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. Access must be immediately removed when a staff changes job duties or leaves the employment.

Authentication Process

Authentication is the process of verifying the identity of a user. Authentication is performed by having the user enter a user name and password in order to access the system.

To help protect information from unauthorized access or disclosure, users must be identified and authenticated per the table below prior to accessing confidential or sensitive information, initiating transactions, or activating services.

Publicly available information such as the mother's maiden name, birth date, and address as the sole authenticator is not a secure means of authentication and should not be used.

Automatic user logons are prohibited. Device-to-device logons must be secured (preferably using client certificates or password via tunneled session). For certain implementations, source restrictions (sign-on can occur only from a specific device) provide a compensating control, in addition to the ID and password.

Authentication information (e.g., a password or PIN) must never be disclosed to another user or shared among users.

The authentication process is limited to three (3) unsuccessful attempts and must be reinstated by the authorized personnel (preferably the System security Administrator). User accounts should be systematically disabled after 90 days of inactivity and must be deleted after 1 year of inactivity

Password Requirements

The purpose of a password is to authenticate a user accessing the system and restrict use of a userID only to the assigned user. To the extent that the functionality is supported within the technology or product, the controls listed must be implemented.

These following controls or content rules apply at any point where a new password value is to be chosen or assigned. These rules must be enforced automatically as part of a new password content checking process:

Password Property	Value
Minimum Length	8 characters with a combination of alpha, numeric and

	special characters
Composition	<ul style="list-style-type: none"> At least two numeric characters (0 through 9), neither of which may be at the beginning or the end of the password A combination of two upper (A through Z) and lower case (a through z) letters Special characters (!, @, #, \$, %, ^, &, *, (,), +, =, /, <, >, ?, ,, : , ; , \) UserID in password is not allowed
Expiration Requirement (Maximum Password Age):	30 days
Revocation	Passwords should be revoked after three (3) failed attempts. (Treasury strongly supports password revocation after three failed attempts if system allows) Passwords should be systematically disabled after 90 days of inactivity to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.
Temporary passwords	<ul style="list-style-type: none"> Must be randomly chosen or generated System must force the user to change the temporary password at initial login
Change process	<p>System must force user to:</p> <ul style="list-style-type: none"> Confirm their current password/PIN, Reenter current password/PIN Create a new password/PIN Reenter new password/PIN <p>System must prevent users from being able to consecutively change their password value in a single day (The goal is to prevent recycling through password history records to reuse an earlier-used password value)</p>
Login process	Password/PIN must not appear on the screen during the login process (The exception to this is during selection of a machine-generated password).
Encryption of passwords/PINs	Passwords must be stored and transmitted with a minimum of 128-bit encryption. Passwords must be masked when entered on any screen
Compromise of password/PIN	Must be changed immediately
Forgotten password/PIN	Must be reset by authorized person (system Security Administrator)
Current user password/PIN	Must not be maintained or displayed in any readable format on the system
Audit logs	Maintain a record of when a password was changed, deleted, or revoked. The audit trail shall capture all unsuccessful login and authorization attempts for a one year period.
Password history	Keep a password history and perform a check against the

	history to verify the password has not been used for a minimum of one year
Privileged account access (e.g. supervisor or root)	Security administrator must change the password for that account immediately when user changes responsibilities

I. System Security Application Control

Application controls apply to individual computer systems and may include such controls as data origin, input controls, processing controls, output controls, application access controls, application interfaces, audit trail controls, and system documentation. Application controls consist of mechanisms in place over each separate computer system to ensure authorized data is processed completely, accurately, and reliably. The contractor is responsible for ensuring application controls are in place and functioning properly within their organization. Ongoing testing and reporting of controls must be part of the business process in order to have a solid understanding of risks, strengths and weaknesses. A comprehensive solution is required to ensure that business critical applications are handled efficiently and are prioritized. Dynamic recovery procedures and fail over facilities shall be incorporated into the scheduling process whenever possible; and where manual processes are needed, extensive tools must be available to minimize delays and ensure critical services are least impacted.

J. System Auditing

The Contractor must (i) create, protect, and retain information system audit log records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

The Contractor must observe the following guidelines regarding system auditing:

1. Audit record should contain the following:
 - a. date and time of the event
 - b. subject identity
 - c. type of event
 - d. how data changed
 - e. where the event occurred
 - f. outcome of the event.
2. System alerts if audit log generation fails
3. System protects audit information from unauthorized access
4. Audit record should be reviewed by individuals with a “need to know” on a regular basis
5. Audit logs are retained for sufficient period of time.

K. Configuration Control and Management

The configuration management policy and procedures must be consistent with applicable federal laws, directives, policies, regulations, standards and guidance.

L. Incident Reporting

1. The Contractor must immediately notify any security incidents and/or breaches to the Program Manager/CCI [see Exhibit 2, Form 4621 What is an Incident? (brochure)].
2. The Contractor must have a documented and implemented Incident Response Policy and Procedure
3. The Contractor must have an incident handling form for consistent, repeatable process for monitoring and reporting when dealing with incidents.
4. The Contractor must have an incident response resource identified to assist users in handling and reporting incidents.
5. Personnel trained in their incident response roles and responsibilities at least annually.

M. Physical and Environmental Security

The Contractor must have established physical and environmental security controls to protect systems, the related supporting infrastructure and facilities against threats associated with their physical environment.

1. The Contractor must have established environmental protection for magnetic and other media from fire, temperature, liquids, magnetism, smoke, and dust.
2. The Contractor must control all physical access points to facilities containing information systems (except those areas within the facilities officially designated as publicly accessible), review physical security logs periodically, investigate security violations or suspicious physical access activities, and initiate remedial actions.
3. The Contractor must periodically review the established physical and environmental security controls to ensure that they are working as intended.

N. Disaster Recovery and Business Continuity Plan

The Contractor must have developed, periodically update, and regularly test disaster recovery and business continuity plans designed to ensure the availability of Department of Treasury's data in the event of an adverse impact to the contractors information systems due to a natural or man-made emergency or disaster event.

O. Security Awareness Training

The Contractor must ensure their staff having access to Treasury information are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security identified in Section A of this document, and ensuring that personnel are trained to carry out their assigned information security related duties.

Contracted employees must obtain Department of Treasury provided security awareness training. (On-line training to be identified by the Program Manger/CCI).

P. Web Application Security

The Contractor shall have established adequate security controls for web application(s) to provide a high level of security to protect confidentiality and integrity of personal, confidential and sensitive data. The controls include, but are not limited to:

1. Secure coding guidelines to ensure that applications are not vulnerable to, at a minimum, the following:
 - Injection flaws, particularly SQL injection, OS command injection, LDAP and Xpath injections
 - Buffer overflow
 - Insecure cryptographic storage
 - Insecure communications
 - Improper error handling
 - Cross-site scripting (XSS)
 - Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)
 - Cross-site request forgery (CSRF).
2. Authentication
3. Authorization and access control
4. Web application and server configuration (e.g., patch management, deletion of unnecessary services, separation of the operating system and the web server)
5. Session management (e.g., randomly generate unique session IDs, encrypt sessions, enforce session expiration date, establish time-out setting for inactive session)
6. Input validation (e.g., avoid shell commands, system calls, and malicious codes),
7. Encryption (e.g., personal, confidential and sensitive data, encryption keys, passwords, shared secret),
 - a. The system shall use SSL (128 bit or higher) for secure communication between the user's browser and the system. SSL will be utilized for:
 - i. Log-on process (authentication information -UserID and passwords)
 - ii. Specific field in the HTML forms and links (URLS) within the pages.
 - iii. Cookies
 - iv. Session id
 - v. Confidential and sensitive data files
 - vi. Encryption keys, certificates, and passwords
 - vii. Audit log file.

8. Audit logs (e.g., all authentication and authorization events, logging in, logging out, failed logins).

EXHIBIT 2**SAFEGUARD REQUIREMENTS OF CONFIDENTIAL DATA**

This (Exhibit) sets forth the safeguard requirements for handling, storage, and processing of confidential tax information for a Contractor and their subcontractor(s) and is incorporated as an integral part of the Contract. It will facilitate administration and enforcement of the laws of the State of Michigan in a manner consistent with the applicable statutes, regulations, published rules and procedures or written communication.

I. Authority

Authority for the Michigan Department of Treasury to require that this section be included in the Contract is contained in 1941 PA 122, as amended, MCL 205.28(1)(f), which subjects current or former contractors to the same restrictions and penalties imposed upon department employees regarding the treatment of confidential information. A private contractor or its employees are strictly prohibited from disclosing taxpayer information to a third party. The prohibition against disclosure does not bar an employee of a private contractor with whom the State of Michigan (State) contracts that processes tax returns or payments pursuant to the Contract from having access to confidential information that is reasonably required for the processing or collection of amounts due this State. Private contractors and any subcontractors will follow Treasury guidelines for Authorized representatives.

II. Confidentiality

It is agreed that all information exchanged under this section will be kept confidential in accordance with the confidentiality provisions contained in the Revenue Act, MCL 205.28(1)(f)-which states in part;

“Except as otherwise provided in this subdivision, an employee, authorized representative, or former employee or authorized representative of the department or anyone connected with the department will not divulge any facts or information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the department for a tax administered by the department.”

Confidential information obtained under this agreement will not be disclosed except as required by state law, or in the proper administration of applicable laws, promulgated rules and procedures. In the event, confidentiality statutes are amended, Treasury will notify Contractor of any changes. No employee, agent, authorized representative or legal representative of Contractor will disclose any information obtained by virtue of this section to any other division within their company or any other governmental agency, department or unit within such governmental agency whether local, state, federal or foreign, department or unit within such governmental agency, or any unauthorized third party. No tax returns or tax return information accessed by Contractor will be duplicated or disseminated within or outside the company without the written approval of the Contract Compliance Inspector. Tax returns and tax return information remain the property of Treasury.

Contractor may use a taxpayer's name, address and Social Security number or employer identification number to the extent necessary in connection with the processing and mailing of forms for any report or return required in the administration of any tax in the performance of the Contract. The use of the Social Security number must be in accordance with the state Social Security Number Privacy Act 454 of 2004, as amended.

Confidential information obtained under this agreement will not be disclosed in part of a report or document that is subject to FOIA.

The penalties for violating the confidentiality provisions of the Revenue Act are contained in, MCL 205.28(2) and MCL 205.27(4). MCL 205.28(2) states:

“A person who violates subsection (1)(e), (1)(f), (4) or (5) is guilty of a felony, punishable by a fine of not more than \$5,000.00, or imprisonment for not more than 5 years, or both, together with the costs of prosecution. In addition, if the offense is committed by an employee of this state, the person will be dismissed from office or discharged from employment upon conviction.”

MCL 205.27(4) states:

A person who is not in violation pursuant to subsection (2), but who knowingly violates any other provision of this act, or of any statute administered under this act, is guilty of a misdemeanor, punishable by a fine of not more than \$1,000.00, or imprisonment for not more than 1 year, or both.

Information received by Treasury from the U.S. Internal Revenue Service, pursuant to section 6103(d) of the Internal Revenue Code or any other federal agency will not be subject to the exchange.

III. Procedure for Security

Contractor will safeguard any tax return information obtained under the Contract as follows:

- A. Access to the tax returns and tax return information will be allowed only to those authorized employees and officials of Contractor who need the information to perform their official duties in connection with the uses of the information authorized in this Contract.
- B. Any records created from tax returns and tax return information will be stored in an area that is physically safe from access by unauthorized persons during duty hours and locked in a secure area during non-duty hours, or when not in use.
- C. Any records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner in which will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of a computer, remote terminal or other means.
- D. All personnel who will have access to the tax returns and tax return information and to any records created by the tax return information will be advised annually of the confidential nature of the information, the safeguards required to protect the information and the civil and criminal sanctions for noncompliance contained in MCL 205.28 (2) and MCL 205.27(4) and will sign confidentiality certifications.
- E. All confidential information, electronic and paper, will be secured from unauthorized access and with access limited to designated personnel only. State tax return information will not be commingled with other information. All Michigan tax returns and return information will be marked as follows: **CONFIDENTIAL - DO NOT DISCLOSE - MICHIGAN TREASURY TAX RETURN INFORMATION**
- F. Treasury, Office of Privacy and Security or Contract Compliance Inspector may make onsite inspections or make other provisions to ensure that adequate safeguards are being maintained by the Contractor.
- G. The Treasury Office of Privacy and Security may monitor compliance of systems security requirements during the lifetime of the Contract or any extension.
- H. Contractor will also adopt policies and procedures to ensure that information contained in their respective records and obtained from Treasury and taxpayers will be used solely as stipulated in the Contract.

IV. Computer System Security of Tax Data

The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

Computer system security and physical security of tax data stored and processed by Contractor must be in compliance with the following security guidelines and standards established by Treasury. These guidelines apply to any computer system developed by Contractor, either through its own systems staff, or through a contractor, subcontractor or vendor):

A. Controlled Access Protection

All computer systems processing, storing and transmitting Michigan tax information must have computer access protection controls. These security standards are delineated in the National Institute of Standards and Technology (NIST) Special Publications number 800-53 “Recommended Security Controls for the Federal Information Systems” at <http://csrc.nist.gov/publications/PubsSPs.html>. To meet these standards, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation.

- 1) **Security Policy** – A security policy is a written document describing the system in terms of categories of data processed, users allowed access and access rules between the users and the data. Additionally, it describes procedures to prevent unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system. Further protection must be provided where the computer system contains information for more than one program/project, office, or Agency and that personnel do not have authorization to see all information on the system.
- 2) **Accountability** – Computer systems processing Michigan tax information must be secured from unauthorized access. All security features must be available (audit trails, identification and authentication) and activated to prevent unauthorized users from indiscriminately accessing Michigan tax information. Everyone who accesses computer systems containing Michigan tax information is accountable. Access controls must be maintained to ensure that unauthorized access does not go undetected. Computer programmers and contractors who have a need to access databases, and are authorized under the law, must be held accountable for the work performed on the system. The use of passwords and access control measures must be in place to identify who accessed protected information and limit that access to persons with a need to know.
 - a) **On-line Access** –Users will be limited to any Treasury on-line functions, by limiting access through functional processing controls and organization restrictions.

Any employee granted access privileges through the Contractor’s Security Administrator will be approved for access and viewing rights to Treasury on-line systems by the Department of Treasury, Office of Privacy and Security.

b) Operating Features of System Security

Contractor must meet the following levels of protection with respect to tax return information. Individual user accountability must be ensured through user identification number and password.

- i. Access rights to confidential tax information must be secured through appropriate levels of authorization.
- ii. An audit trail must be maintained of accesses made to confidential information.
- iii. All confidential and protected information must be cleared from a system before it is used for other purposes not related to the enforcement, collection or exchange of data not covered by this section or by an addendum to this Contract.

- iv. Hard copies made of confidential tax return information must be labeled as confidential information.
- v. Confidential Treasury tax information will be blocked or coded as confidential on system.
- vi. Any computer system in which Michigan tax return information resides must systematically notify all users upon log-in of the following disclosure penalties for improperly accessing or making an authorized disclosure of Michigan tax return information:

NOTICE TO STATE AGENCY EMPLOYEES AND AUTHORIZED REPRESENTATIVES

This system contains Michigan Department of Treasury tax return information. **DO NOT DISCLOSE OR DISCUSS MICHIGAN RELATED TAX RETURN INFORMATION** with unauthorized individuals. The Revenue Act at MCL 205.28(1)(f) prohibits such disclosure.

MICHIGAN PENALTIES

A person making a willful unauthorized disclosure or inspection (browsing) of tax return information may be charged with the following Michigan penalties:

- Criminal penalties up to \$5,000 and/or imprisonment for 5 years, plus costs and dismissal from employment if it is found that a current or former employee or authorized representative has made an unauthorized disclosure of a tax return or tax return information or divulged audit selection or processing parameters. [MCL 205.28(2)]
- A misdemeanor, punishable by a fine of not more than \$1,000.00, or imprisonment for not more than 1 year, or both if the person is not in violation pursuant to MCL 205.27(2), but who knowingly violates any other provision of this act, or of any statute administered under this act.

This statement is subject to modification. A confidentiality statement, subject to modification, will be sent as needed by the Security Administrator to all employees, contractors, and legal representatives of Contractor.

- 3) **Assurance** – Contractor must ensure that all access controls and other security features are implemented and are working when installed on their computer system. Significant enhancements or other changes to a security system must follow the process of review, independent testing, and installation assurance. The security system must be tested at

least annually to assure it is functioning correctly. All anomalies must be corrected immediately.

- a) The Contractor must initiate corrective action for all non-conformities as soon as detected and immediately advise the Contract Compliance Inspector. Notice of the corrective action must be provided to the Contract Compliance Inspector. All non-conformities must be reported to the Contract Compliance Inspector with the following:
 - a. Duration of non-conformity/interruption
 - b. Reason for non-conformity/interruption
 - c. Resolution.
 - b) All non-conformities to the specifications/tasks of the Contract must be corrected within four (4) hours. The State recognizes there will be instances when adherence to this time frame will not be possible. However, the State will only tolerate this on an exception basis. To request an exception to this time frame, the Contractor must submit a detailed project plan to address the non-conformity within four (4) hours to the Contract Compliance Inspector for approval.
- 4) **Documentation** – Design and test documentation must be readily available to the state. The developer or manufacturer should initially explain the security mechanisms, how they are implemented and their adequacy (limitations). This information should be passed on to the security officer or supervisor. Test documentation should describe how and what mechanisms were tested and the results. If recognized organizations/tests/standards are used, then a document to that effect will suffice. For example, a system that has been tested and certified as meeting certain criteria may have a document stating this fact, without detailed tests/results of information. Contractor, however, must ensure the documentation covers the exact system and that it includes the specific computer system used by Contractor.

Additionally, documentation must include a security administrator's guide. The security administrator's guide is addressed to the System's Administrator and Security Officer and will describe the protection mechanisms provided by the security system, guidelines on their use and how they interact. This document will present cautions about security functions and describe privileges that should be controlled when running a secure system. The document will be secured and locked at all times with access rights only by the Systems Administrator and Security Officer.

Note: When a security system is designed or purchased for a specific computer or computer system, the security mechanisms must be reviewed by the State to ensure that needed security parameters are met. An independent test should be implemented on the specific computer or computer system to ensure that the security system meets the security parameters within this contract and developed with the computer system. The test may be arranged by the developer but must be done by an independent organization. Contractor must assign responsible individuals (Security Officers) with knowledge of information technology and applications to oversee the

testing process. These individuals must be familiar with technical controls used to protect the system from unauthorized entry.

Finally, contingency and backup plans must be in place to ensure protection of Michigan tax information.

V. Electronic Transmission of Michigan Tax Information

The two acceptable methods of transmitting Michigan tax information over telecommunications devices are encryption and using guided media. Encryption involves altering data objects in a way that the objects become unreadable until deciphered with the appropriate software at the intended destination. Guided media involves transmission of data over twisted pair cable, coaxial cable or end to end fiber optics which are typically used in secure computer networks like the state's Local Area Network (LAN), telephone systems, and television distribution.

Cryptography standards have been adopted by the IRS and can be used to provide guidance for encryption, message authentication codes or digital signatures and digital signatures with or without an associated certification infrastructure. For further information, see IRS Publication 1075 at the IRS web site.

Unencrypted cable circuits of fiber optics are an acceptable alternative for transmitting Michigan tax information. Adequate measures must be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio or microwave transmission. Additional precautions should be taken to protect the cable, i.e., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers.

A. Remote Access

Accessing databases containing Michigan tax information from a remote location – that is, a location not directly connected to the Local Area Network (LAN) will require adequate safeguards to prevent unauthorized entry.

For remote access, the contractor is required to use an identification security card that requires both PIN and card in possession. The Sate identified and approved methods for remote vendor access are as follows:

- SecureID through VPN – Sate provided SecureID taken and VPN software in order to access State of Michigan resources. Appropriate Acceptable Use policies and signoffs are required
- Follow-the Sun SecureID – Vendor is provided with VPN software and a SOM technical resource coordinates with the DTMB Client Service Center to provide secure ID code access to specific State of Michigan resources. Appropriate Acceptable Use Policies and signoffs are required.

B. Portable Computer Devices

Any entrusted confidential information collected or accessed during this Contract must be encrypted when stored on all storage devices and media. This includes, but not limited to,

disk drives for servers and workstations, and portable memory media (PDAs, RAM drives, memory sticks, etc.).

VI. Record Keeping Requirements for Information Received

Each Contractor, requesting and receiving information will keep an accurate accounting of the information received. The audit trail will be required which will include the following information:

- a. Taxpayer's name
- b. Identification number
- c. Information requested
- d. Purpose of disclosure request
- e. Date information received
- f. Name of Agency/Division and employee making request
- g. Name of other employees who may have had access
- h. Date destroyed
- i. Method of destruction

The Contractor will adopt and implement formal procedures to:

- Ensure proper handling of tax returns and tax return information;
- Secure and safeguard information from unauthorized use; and
- Ensure appropriate destruction of information and materials retrieved from Treasury.

A. Electronic Media

Contractor will keep an inventory of magnetic and electronic media received under the Contract.

Contractor must ensure that the removal of tapes and disks and paper documents containing Michigan tax return information from any storage area is properly recorded on charge-out records. Contractor is accountable for missing tapes, disks, and paper documents.

B. Recordkeeping Requirements of Disclosure Made to State Auditors

When disclosures are made by Contractor to State Auditors, these requirements pertain only in instances where the Auditor General's staff extracts Michigan tax returns or tax information for further review and inclusion in their work papers. Contractor must identify the hard copies of tax records or if the tax information is provided by magnetic tape format or through other electronic means, the identification will contain the approximate number of taxpayer's records, the date of inspection, the best possible description of the records and the name of the Auditor(s) making the inspection.

The Disclosure Officer must be notified, in writing, of any audits done by auditors, internal or otherwise, of Contractor that would involve review of Treasury processing parameters.

VII. Contract Services

To the extent the Contractor employs an independent agency, consultant, or agent to process confidential information which includes Michigan tax return information; the Contractor will notify the Treasury Disclosure Officer before the execution of any such agreement. Each agreement will include in the agreement the following recommended safeguard provisions:

A. The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

B. Definition of Treasury Tax Return Information as defined in Revenue Administrative Bulletin (RAB) 1989-39:

Taxpayer's identity, address, the source or amount of his/her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments whether the taxpayer's return was, is being or will be examined or subject to their investigation or processing, or any other data, received by, recorded by, prepared by, furnished to or collected by the agency with respect to a return or with respect to the determination of the existence, or liability (or the amount thereof) of any person under the tax laws administered by the Department, or related statutes of the state for any tax, penalty, interest, fine, forfeiture, or other imposition or offense. The term "tax return information" also includes any and all account numbers assigned for identification purposes.

C. An acknowledgment that a taxpayer has filed a return is known as a "fact of filing" and may not be disclosed. All tax return data made available in any format will be used only for the purpose of carrying out the provisions of the Contract between Contractor and the subcontractor. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract between Contractor and the subcontractor. In addition, all related output will be given the same level of protection as required for the source material.

D. The subcontractor will certify that the data processed during the performance of the Contract between Contractor and the subcontractor will be completely purged from all data storage components of the subcontractor's computer facility, and no output will be retained by the subcontractor at the time the work is completed.

E. Destruction of tax data, including any spoilage or any intermediate hard copy printout which may result during the processing of Michigan tax return information, will be documented with a statement containing the date of destruction, description of material destroyed, and the method used. Destruction parameters must meet the standards of Section IX, Disposal of Tax Information, of this agreement.

F. Computer system security and physical security of tax data stored and processed by the subcontractor must be in compliance with security guidelines and standards established by this contract. See section VI (Record Keeping Requirements for Information Received in Paper Format) for more details.

- G. The Contractor will be responsible for maintaining a list of employees authorized to access Michigan tax return information and will provide a copy of such list to Treasury.
- H. No work involving information furnished under the contract will be subcontracted without the specific approval of Treasury. Contractor and approved subcontractors handling Michigan tax return information will be required to sign the *Vendor, Contractor or Subcontractor Confidentiality Agreement* provided by Treasury, (Form 3337, see Attachment A). The original agreements will be returned to the Disclosure Officer for the Department of Treasury and a copy sent to the Contract Compliance Inspector.

VIII. Transport of Tax Information

In the event, it is necessary to transport confidential tax return information the Contractor is responsible for holding the carrier responsible for safeguarding the records.

The Contractor must obtain a signed *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A) for each carrier employee who has access to Michigan tax return information. The original agreements will be returned to the Department of Treasury, Disclosure Officer and a copy sent to the Contract Compliance Inspector.

If it is necessary to transfer records and responsibility for transport to a third carrier due to a mishap during transportation, the Contractor is responsible for ensuring safeguard standards remain enforce. This type of incident will be documented in accordance with the incident reporting guidelines in procedure PT-03253, "Incident Reporting and Handling".

Any such incidents must be reported to the Contract Administrator immediately.

IX. Disposal of Tax Information

Materials furnished to Contractor, such as tax returns, remittance vouchers, W-2 reports, correspondence, computer printouts, carbon paper, notes, memorandums and work papers will be destroyed by burning, mulching, pulverizing or shredding. If shredded, strips should not be more than 5/16-inch, microfilm should be shredded to affect a 1/35-inch by 3/8-inch strip, and pulping should reduce material to particles of one inch or smaller.

data tracks should be overwritten or reformatted a minimum of three times or running a magnetic strip over entire area of disk at least three (3) times to remove or destroy data on the disk media Electronic data residing on any computer systems must be purged based on Treasury's retention schedule.

Contractor and its subcontractor(s) will retain all confidential tax information received by Treasury only for the period of time required for any processing relating to the official duties and then will destroy the records. Any confidential tax information that must be kept to meet evidentiary requirements must be kept in a secured, locked area and properly labeled as confidential return information. See Procedure for Security (Section III of this agreement) for more details.

X. Security Responsibility

Contractor will designate a security person who will ensure that each individual having access to confidential tax information or to any system which processes Michigan tax return information is appropriately screened, trained and executes a *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A) before gaining access or transaction rights to any process and computer system containing Treasury tax return information.

Each Contractor or their subcontractor(s) employees' access and transaction rights will be reviewed periodically to ensure that there is a need to know Treasury tax return information displayed in any media.

Michigan tax return information will be made available only to individuals authorized by the Contract. Contractor will maintain a list of persons authorized to request and receive information and will update the list as necessary. A copy of the list must be furnished to the Michigan Department of Treasury Disclosure Officer and Contract Compliance Inspector.

Treasury and the Agency anticipate that there may be changes to the titles and/or responsibilities of officers and employees designated within this Agreement. In the event of such changes, any actions that may be taken under this Agreement by said officers or employees may be taken by any officer(s) or employee(s) Treasury and the Agency respectively determine to have succeeded to the relevant portions of said officers or employees authorities or responsibilities.

XI. Security Breach Notification

The Agency agrees to report to Treasury, on Form 4000, Incident Reporting (Attachment B) any use or disclosure of confidential information, whether suspected or actual, immediately after becoming aware of the use or disclosure. The Agency may substitute its internal form for Form 4000 if all pertinent information is included.

The Agency agrees to immediately contain the breach if it is determined ongoing.

Treasury has the right to terminate the Agreement when a breach has occurred and the Agency cannot demonstrate proper safeguards were in place to avert a breach. Treasury must approve Agency's resolution to the breach.

XIII. Certification of Compliance

In accordance with this Agreement, the Contractor will fully protect State Tax Information (STI) entrusted to them. Each Contractor or subcontractor who will have access to STI must read and sign a confidentiality agreement. This agreement requires that all information obtained from the Michigan Department of Treasury under the Revenue Act, PA 122 of 1941, MCL 205.28 (1)(f) be kept confidential. In the event of a security breach involving STI in the possession of the Agency, the Agency agrees to provide full cooperation to conduct a thorough security review. The review will validate compliancy with the agreement, and state laws and regulations.

If, as a result of the Contractor's failure to perform as agreed, the State is challenged by a governmental authority or third party as to its conformity to or compliance with State, Federal

and local statutes, regulations, ordinances or instructions; the Contractor will be liable for the cost associated with loss of conformity or compliance.

The Contractor understands the cost reflects violation fines identified by the Michigan Social Security Number Privacy Act, 454 of 2004 and the Michigan Identity Theft Protection Act, Act 452 of 2004 as amended.

XI. Effective Date

These Safeguard requirements will be reviewed whenever the Contract modifications include specifications or processes that affect tax data.

Attachment A

Form 3337, Vendor, Contractor or

Michigan Department of Treasury
3337 (Rev. 01-12)

Vendor, Contractor or Subcontractor Confidentiality Agreement

The Revenue Act, Public Act 122 of 1941, MCL 205.28(1)(f), makes all information acquired in administering taxes confidential. The Act holds a vendor, contractor or subcontractor and their employees who sell a product or provide a service to the Michigan Department of Treasury, or who access Treasury data, to the strict confidentiality provisions of the Act. Confidential tax information includes, but is not limited to, information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the Michigan Department of Treasury for a tax administered by the department.

INSTRUCTIONS. Read this entire form before you sign it. If you do not complete this agreement, you will be denied access to Michigan Department of Treasury and federal tax information. After you and your witness sign and date this form, keep a copy for your records. Send the original to the address listed below.

Company Name and Address (Street or RFR, City, State, ZIP Code)		Last Name	First Name
		Driver License Number/Passport Number	Telephone Number
State of Michigan Department	Division	Subcontractor Name if Product/Service Furnished to Contractor	
Describe here or in a separate attachment the product or service being provided to the State of Michigan Agency (Required).			

Confidentiality Provisions. It is illegal to reveal or browse, except as authorized:

- All tax return information obtained in connection with the administration of a tax. This includes information from a tax return or audit and any information about the selection of a return for audit, assessment or collection, or parameters or tolerances for processing returns.
- All Michigan Department of Treasury or federal tax returns or tax return information made available, including information marked "Official Use Only". Tax returns or tax return information shall not be divulged or made known in any manner to any person except as may be needed to perform official duties. Access to Treasury or federal tax information, in paper or electronic form, is allowed on a need-to-know basis only. Before you disclose returns or return information to other employees in your organization, they must be authorized by Michigan Department of Treasury to receive the information to perform their official duties.
- Confidential information shall not be disclosed by a department employee to confirm information made public by another party or source which is part of any public record. 1999 AC, R 2005.1004(1).

Violating confidentiality laws is a felony, with penalties as described:

Michigan Penalties

MCL 205.28(1)(f) provides that you may not willfully browse any Michigan tax return or information contained in a return. Browsing is defined as examining a return or return information acquired without authorization and without a need to know the information to perform official duties. Violators are guilty of a felony and subject to fines of \$5,000 or imprisonment for five years, or both. State employees will be discharged from state service upon conviction.

Any person who violates any other provision of the Revenue Act, MCL 205.1, et seq., or any statute administered under the Revenue Act, will be guilty of a misdemeanor and fined \$1,000 or imprisonment for one year, or both, MCL 205.27(4).

Federal Penalties

If you willfully disclose federal tax returns or tax return information to a third party, you are guilty of a felony with a fine of \$5,000 or imprisonment for five years, or both, plus prosecution costs according to the Internal Revenue Code (IRC) §7213, 26 USC 7213.

In addition, inspecting, browsing or looking at a federal tax return or tax return information without authorization is a felony violation of IRC §7213A, subjecting the violator to a \$1,000 fine or imprisonment for one year, or both, plus prosecution costs. Taxpayers affected by violations of §7213A must be notified by the government and may bring a civil action against the federal government and the violator within two years of the violation. Civil damages are the greater of \$1,000 or actual damages incurred by the taxpayer, plus the costs associated with bringing the action, 26 USC 7431.

Failure to comply with this confidentiality agreement may jeopardize your employer's contract with the Michigan Department of Treasury.

Certification		
By signing this Agreement, I certify that I have read the above confidentiality provisions and understand that failure to comply is a felony.		
Print name of employee signing this agreement	Signature of person named above	Date signed
Print Witness Name (Required)	Signature of Witness (Required)	Date signed

Submit your form to the following address:

Office of Privacy and Security/ Disclosure Unit
Michigan Department of Treasury
430 W. Allegan Street
Lansing, MI 48922

Questions, contact the Office of Privacy and Security by telephone, (517) 636-4239; fax, (517) 636-5340; or email: Treas_Disclosure@michigan.gov

Attachment B
Form 4000, Incident Reporting

Reset Form

Incident Report

INSTRUCTIONS: Complete Parts 1 and 2 and immediately submit Initial Report to the Office of Privacy and Security. After incident resolution, submit Final Report (Parts 1, 2 and 3) to the Office of Privacy and Security. Refer to Procedure PT-03253, Incident Reporting and Handling.

PART 1: A. CONTACT INFORMATION (Reporting Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
Telephone Number	Fax Number	E-Mail Address	
B. CONTACT INFORMATION (Affected Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
Telephone Number	Fax Number	E-Mail Address	
PART 2: INCIDENT INFORMATION			
Whose information was involved in the incident? <input type="checkbox"/> Treasury <input type="checkbox"/> Federal Tax Information <input type="checkbox"/> Other State Agency, specify _____ <input type="checkbox"/> Other _____			
Incident Category (select all that apply)			
<input type="checkbox"/> Passwords Shared/Stolen	<input type="checkbox"/> Computer Virus/Spam	<input type="checkbox"/> Paper Archives Compromised	
<input type="checkbox"/> Misrouted Communications	<input type="checkbox"/> Data Destruction/Deletion	<input type="checkbox"/> Safe/Lockbox/other Compromise	
<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> Backups Missing or Stolen	<input type="checkbox"/> Delivery of Documents Lost	
<input type="checkbox"/> Fraudulent Actions	<input type="checkbox"/> Hacking of Networks/Systems	<input type="checkbox"/> Inappropriate Destruction Paper	
<input type="checkbox"/> Lost/Stolen Information/Data	<input type="checkbox"/> Improperly Secured Sys/Web	<input type="checkbox"/> Inappropriate Destruction Media	
<input type="checkbox"/> Lost/Stolen Cash/Checks	<input type="checkbox"/> Circumvention of Security Protocols	<input type="checkbox"/> Lost/Stolen Equipment	
<input type="checkbox"/> Inappropriate Building Access	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
Incident Affects			
<input type="checkbox"/> Financial Information/Resources	<input type="checkbox"/> Personal Information (SSN, Driver License No. Financial information)	<input type="checkbox"/> Unauthorized/Unlawful Activity	
<input type="checkbox"/> Confidential/Sensitive Information	<input type="checkbox"/> Human Resources (threat)	<input type="checkbox"/> Other _____	
Date Incident Occurred	Time Incident Occurred	Date Incident Discovered	Time Incident Discovered
Incident Location		Number of Individuals Affected	
Involved Parties/Entities		Does this involve personal information (first and last name along with a SSN, driver license number, or credit/debit card account number)? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Date of Initial Report			
Description of Incident			

PART 1: CONTACT INFORMATION (Affected Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
PART 3: INCIDENT RESOLUTION			
Notification issued to affected individuals? <input type="checkbox"/> Yes <input type="checkbox"/> No		How many notifications were sent?	Breach Notification Method? <input type="checkbox"/> E-mail <input type="checkbox"/> Telephone <input type="checkbox"/> US Mail <input type="checkbox"/> Web
Who was notified?		Date notification was issued	
Incident Cost <input type="checkbox"/> Check if incident costs are less than \$250. If \$250 or more, complete the detailed summary of costs below.			
<u>Manhours:</u> Treasury \$ _____ DTMB-OES \$ _____ DTMB-Treasury Agency Services \$ _____		<u>Other:</u> Postage \$ _____ Credit Monitoring Service \$ _____ _____ \$ _____ Total Cost of Incident \$ _____	
Action Taken			
Incident Impact			
Post Incident Recommendations			
PART 4: REPORT PREPARER INFORMATION			
Final Report Prepared By:		Date Prepared	Preparer Title
Preparer Signature			Preparer's Telephone Number
			Date
OFFICE OF PRIVACY AND SECURITY USE ONLY			
Administrator, Office of Privacy and Security Signature			Date