STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **210000001333**
between
THE STATE OF MICHIGAN
and

	Cisco Systems, Inc.
	170 West Tasman Drive
	San Jose, CA 95314
	Gigi Feril
	(408) 424-0712
	nvp-help@cisco.com
	CV0063483

STATE	Program Manager	Ashley Adrian	DTMB
		517-331-4622	
		Adriana1@michigan.gov	
	Contract Administrator	KeriAnn Trumble	DTMB
		989-259-2625	
		Trumblek1@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Data Communications Products and Services			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
8/10/2021	09/30/2024	2 – 1 Year	09/30/2026
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☒ P-card ☐ Payment Request (PRC) ☐ Other			☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
This Contract is being established as a Participating Addendum to the NASPO ValuePoint Master Agreement # AR3227. This solicitation was led by the State of Utah and is available to all NASPO Participants.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$ 75,000,000.00**

FOR THE CONTRACTOR:

Cisco Systems, Inc.

Company Name

E-SIGNED by Jenn Pate
on 2021-08-12 13:07:15 EDT

Authorized Agent Signature

Jenn Pate

Authorized Agent (Print or Type)

2021-08-12 13:07:15 UTC

Date

FOR THE STATE:

E-SIGNED by Jared Ambrosier
on 2021-08-12 20:41:40 EDT

Signature

Jared Ambrosier CPO

Name & Title

State of Michigan

Agency

2021-08-12 20:41:40 UTC

Date

NASPO ValuePoint

PARTICIPATING ADDENDUM

DATA COMMUNICATIONS PRODUCTS & SERVICES (2019-2026)

Led by the State of **Utah**

Master Agreement #: AR3227

Participating Addendum #: 210000001333

Contractor: **CISCO SYSTEMS, INC.**

Participating Entity: **STATE OF MICHIGAN**

The following products or services are included in this contract portfolio:

- All products and services listed on the Contractor page of the NASPO ValuePoint website and/or Contactor's contract website, except for the products and services listed below that are not included in this agreement.

The following products or services are not included in this agreement:

- Leasing and alternative financing services are not included for the State of Michigan's use but may be used by MiDEAL members.

Master Agreement Terms and Conditions:

1. Scope: This addendum covers the NASPO ValuePoint Master Agreement for ***Data Communications Products Services (2019-2026)*** led by the State of UTAH for use by state agencies and other entities located in the Participating State which is the State of Michigan (the "**State**") authorized by the State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official. "**Participating Addendum**" means this addendum including all amendments and attachments incorporated in Section 4 of this addendum.

2. Participation: This NASPO ValuePoint Master Agreement may be used by all state agencies and other entities authorized to use statewide contracts in the State of Michigan and is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

   If extended to MiDEAL members, Contractor must supply all services, products and deliverables at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions. Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis. MiDEAL members may purchase additional Products and Services including Contractor's lease and alternative financing offerings under this Participating Addendum notwithstanding the fact that such offerings are excluded for state agencies.

3. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Gigi Feril
Address:	170 West Tasman Dr. San Jose, CA 95134
Telephone:	(408) 424-0712
Fax:	(408) 608-1729
Email:	nvp-help@cisco.com

Participating Entity

Name:	KeriAnn Trumble
Address:	State of Michigan DTMB, Central Procurement Services – Enterprise Sourcing Constitution Hall, 1st Floor, NE 525 W. Allegan Street Lansing, MI 48933
Telephone:	(989) 259-2625
Fax:	517-335-0046
Email:	TrumbleK1@michigan.gov

4. Participating Entity Modifications Or Additions To The Master Agreement

These modifications or additions apply only to actions and relationships within the Participating Entity.

Participating Entity must check one of the boxes below.

[___] No changes to the terms and conditions of the Master Agreement are required.

[X] The following changes are modifying or supplementing the Master Agreement terms and conditions. The following attachments are incorporated herein:

- Attachment 1 - State of Michigan Terms and Conditions, which includes:
  - Schedule A – Data Security Schedule (together with Exhibits A, B, and C)
  - Federal Provisions Addendum
- Attachment 2 - State of Michigan ITAM Requirements
- Attachment 3 - Software License Terms and Conditions
- Attachment 4 – Additional Contractor Terms and Conditions

- Attachment 5 – State of Michigan Service Level Agreement
- Attachment 6 – Personal Data Brief

5. Lease Agreements and Alternative Financing Methods: Contractor's Master Agreement which allows for leasing under Section 45 is approved for use by the Participating State's MiDeal members only. The terms and conditions of the capital lease or financing arrangement will be separately negotiated and set forth in an agreement between the purchaser and either Cisco Capital or its designated and/or approved financing partner

6. Subcontractors: Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any third party to perform as a Fulfillment Partner, as defined in the Master Agreement. Once approved by the State, Contractor's Fulfillment Partners, authorized in the State of Michigan, may be shown on the dedicated Contractor's (cooperative contract) website, and are approved to provide sales and service support to Participating Entities, e.g., for direct order taking, processing, fulfillment, or provisioning. The Fulfillment Partners' participation will be in accordance with the terms and conditions set forth in this Participating Addendum, including the State of Michigan Terms and Conditions, and the aforementioned Master Agreement.

   Subject to approval of the State, Contractor may add Fulfillment Partners at any time during the term of this Participating Addendum. Contractor and State agree on adding a minimum of 4 Fulfillment Partners and a maximum number of 11 Fulfilment Partners to provide sales and services support provided that Fulfillment Partners are able to support the State of Michigan's ITAM requirements in Attachment 2. Contractor will add Fulfillment Partners upon the written request of the State provided such Fulfillment Partner meets Contractor's established qualifying criteria and the addition would not violate any state or federal law or regulation. Notwithstanding the foregoing, subject to the written approval of the State, Contractor may remove any Fulfillment Partner who does not meet Contractor's established qualifying criteria The State, in its sole discretion, may require the removal of any Fulfillment Partner. Contractor or its Fulfillment Partners must perform the tasks and meet the requirements of Attachment 2 - State of Michigan ITAM Requirements and Attachment 5 – State of Michigan Service Level Agreement.

7. Orders: The Master Agreement number and the Participating Addendum Number must appear on every Delivery Order or other SIGMA ordering document placed under this Participating Addendum.

   Purchasers may place orders directly only through Contractor's approved Fulfillment Partners or through Contractor (only on an as-needed basis) for products or services as authorized under this Participating Addendum. Only those Fulfillment Partners approved and listed during the term of Participating Addendum at Contractor's website are authorized to directly provide quotes, receive purchase orders, invoice Customers, and receive payment from purchasers on Contractor's behalf.

Except as otherwise set forth in the qualifying criteria, Contractor will not, directly, or indirectly,restrict any Fulfillment Partner's participation or ability to quote pricing for a Customer. The approved Fulfillment Partners will not offer less favorable pricing discounts than the contract discounts established by Contractor under the Master Agreement. However, the Fulfillment Partner may offer any additional incremental discounts to Participating State/Entity, and such additional discounts if offered, may be provided in the discretion and as the sole legal obligation of the approved Fulfillment Partner to the Participating State/Entity.

Any order placed by a Participating Entity or Purchasing Entity for a product and/or service under this Master Agreement as amended by this Participating Addendum shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement as amended by this Participating Addendum unless the parties to the order agree in writing that another contract or agreement applies to such order. *For clarity, sales of Contractor's product or services by Contractor or an authorized reseller made under a separate contract, where the applicable quoting or ordering documents reference that separate contract, are not deemed to be sales under this Master Agreement as amended by this Participating Addendum*.

8. The Term of this Participating Addendum shall begin on August 10, 2021 ("Effective Date"), and unless earlier terminated, expires on September 30, 2024 (the "Term"). If, pursuant to the terms of Master Agreement #AR3227 the term of the Master Agreement is extended, this Participating Addendum may be renewed by the State for any applicable number of additional one (1) year periods or other length of time that coincides with any such extension of the term of the Master Agreement. Any renewal by the State, including the length of such renewal, is at the sole discretion of the State and will automatically extend the Term of this Participating Addendum. The State will document the exercise of its renewal option(s) via Contract change notice.

9. Notices: Notwithstanding anything contained in the Master Agreement to the contrary, all notices required or permitted under this Participating Addendum will be in writing and will be deemed given: 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 sent by confirmed facsimile or electronic mail. All communications will be sent to the addresses set forth Section 3 of this Participating Addendum (and notices to Cisco shall be further addressed to the Office of the General Counsel, Attn: Contract Notice) or such other address as may be designated by a party by giving written notice to the other party pursuant to this paragraph, or, in the absence of such an address from Customer, to the address to which the last invoice under this Participating Addendum was sent before notice is served.

10. Entire Agreement: This Participating Addendum (including all amendments and attachments hereto) and the Master Agreement (including all amendments and attachments thereto) (collectively, the "Contract") constitute the entire agreement between the parties concerning the subject matter of this Participating Addendum and replaces any prior oral or written

communications between the parties, all of which are excluded. There are no conditions, NASPO ValuePoint understandings, agreements, representations or warranties, expressed or implied, that are not specified herein. The terms and conditions of this Participating Addendum (including all amendments and attachments hereto) shall prevail and govern in the case of any inconsistency or conflict with the terms and conditions of the Master Agreement. Any conflict among the attachments and documents incorporated into this Participating Addendum in Section 4 above shall be resolved by giving priority to those documents in the order listed in Section 4 above. This Contract may be modified only by a written document executed by the parties hereto. UNLESS OTHERWISE SPECIFIED IN THIS PARTICIPATING ADDENDUM, NO TERMS ON CONTRACTOR'S INVOICES, ORDERING DOCUMENTS, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON- NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE CONTRACT SERVICES OR DELIVERABLES WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF THE CONTRACT SERVICES OR DELIVERABLES REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

IN WITNESS, WHEREOF, the parties have executed this Addendum as of the last date of execution by both parties below.

Participating Entity: State of Michigan	Contractor: Cisco Systems, Inc.
Signature: E-SIGNED by Jared Ambrosier on 2021-08-12 20:41:44 EDT	Signature: E-SIGNED by Jenn Pate on 2021-08-12 13:07:27 EDT
Name: Jared Ambrosier	Name: Jenn Pate
Title: CPO	Title: Legal Analyst
Date: 2021-08-12 20:41:44 UTC	Date: 2021-08-12 13:07:27 UTC

Attachment 1 – State of Michigan Terms and Conditions

STATE OF MICHIGAN

STANDARD CONTRACT TERMS

The parties agree as follows:

All initial capitalized terms in this Attachment 1 that are not defined herein shall have the respective meanings given to them in the Participating Addendum or Master Agreement.

Definitions.

"**Authorized User**" has the meaning in the Attachment 3 – Software License Terms and Conditions.

"Business Contact Information" is information about State and Contractor's personnel provided during sign-up, purchase or contracting, or management of products or services. This may include name, business address, business phone number, and business email address, whether collected at the time of the initial agreement or later during management of the products or services.

"**Cloud Software**" means Hosted Services as defined in the attached SCHEDULE A DATA SECURITY Schedule below.

"**Contractor Hosted**" means the Operating Environment is provided by Contractor or one or more of its subcontractors.

"Customer Content" means data such as text, log, configuration, firmware, audio, video or image files or core dumps, provided by the State to Contractor in connection with the State's use of Contractor solutions, and data developed at State's specific request related to a statement of work or contract. Customer Content does not include Systems Information.

"**Customer Feedback**" means technical data or suggestions contained in oral or written communications the State provides to Contractor regarding modifications or improvements to a product or service.

"**De-identified**" or "de-identified" means all uniquely identifiable data related to a user, a user device, or a user location has been removed.

"**Entitlement Information**" means Software license, warranty, cloud, and service subscription information.

"Harmful Code" means, with regards to properly licensed Contractor solutions (meaning purchased through proper channels and/or with valid term licenses) any software, hardware or other technologies, devices or means, the purpose or effect of which is to surreptitiously: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

"**Install Base Information**" means types, quantities and location of installed Cisco devices, products, or software releases.

"**Open-Source Components**" means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

"**Operating Environment**" means, collectively, the platform, environment, and conditions on, in or under which the Software is intended to be installed and operate, including such structural, functional, and other features, conditions and components as hardware,operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

"PAT" means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

"Personal Data" means any information relating to an identified or identifiable natural person. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

"**Security Threat Data**" means threat intelligence data, URLs, metadata, net flow data, origin and nature of malware and other information necessary to enable security features of a product or service.

"**Software**" has the meaning in the NASPO ValuePoint Master Agreement.

"**State Hosted**" means the Operating Environment is not provided by Contractor or one or more of its subcontractors.

"**Support Data**" means data Contractor collects when the State submits a request for support services or other troubleshooting, including information about hardware, software and other details related. to the support incident. Note that Support Data doesnot include data submitted in an attachment to a support request; that data is Customer Content.

"Systems Information" means data generated or collected in connection with the State's use and operation of Contractor solutions, and data provided by the State in connection with Contractor's delivery of products and services to the State (including, for example, when the State submits a request related to support services). Systems Information is composed only of Telemetry Data, Support Data, Install Base Information, Entitlement Information, Customer Feedback and Security Threat Data, as defined further in this Attachment 1. For clarity, Systems Information does not include Customer Content or Personal Data. To the extent any Customer Content or Personal Data is incidentally collected or included with Systems Information, such data will not be considered or treated as Systems Information.

"**Telemetry Data**" means data generated by instrumentation and logging systems created through the use and operation of the product or service.

"WCAG 2.0 Level AA" means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

1. **Duties of Contractor.** Contractor must perform the Services and provide the Products, services, and deliverables described in the Contract, or an applicable Statement of Work (the "**Contract Activities**"). Services, Products, Statement of Work and Master Agreement are each defined in the attached NASPO ValuePoint Terms and Conditions.

   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) obtain and maintain all necessary licenses, permits or other authorizations necessary for the performance of the Contract; (c) 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; (d) not make any media releases without prior written authorization from the State; and (e) 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. **RESERVED.**

3. **Contract Administrator.** The Contract Administrator for each party is the only person authorized to modify any terms of this Contract, and approve and execute any change under this Contract (each a "**Contract Administrator**"):

State:	Contractor:
KeriAnn Trumble - State of Michigan DTMB, Central Procurement Services Enterprise Sourcing Constitution Hall, 1st Floor, NE 525 W. Allegan Street Lansing, MI 48933	Cisco Systems, Inc. Gigi Feril 170 West Tasman Dr. San Jose, CA 95134 nvp-help@cisco.com (408) 424-0712

(989) 259-2625 TrumbleK1@michigan.gov	

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**"):

State:	Contractor:
Ashley Adrian DTMB Infrastructure and Operations (I&O) Network and Telecommunications Services Division (NTSD) 608 W. Allegan St. Lansing, MI 48915 Adriana1@michigan.gov Desk: (517) 284-7454 Cell: (517) 525-9338	Cisco Systems, Inc. Cody Lynch 170 West Tasman Dr. San Jose, CA 95134 nvp-help@cisco.com (604) 647-2343

5. **RESERVED.**

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) (a) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (b) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: $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	The State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents shall be included as additional insureds for liabilities that fall within Contractor's indemnity obligations under this Agreement that are covered by such insurance.
Automobile Liability Insurance	
If a motor vehicle is used in the performance of the Contract, Contractor must maintain motor vehicle liability coverage for bodily injury and property damage, as required by law, for the term of the Contract	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	The policy shall provide that the insurer waives its rights of subrogation against the State.
Employers Liability Insurance	
Minimum Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: $1,000,000 Each Claim $1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

If any of the required policies provide **claims-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 cancelled 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 delivery order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; and (b) notify the Contract Administrator within 5 business days if any insurance is cancelled. The insurance required herein shall provide that the insurers waive their rights of subrogation against the State for liabilities that fall within Contractor's indemnity obligations under this Agreement. If contractor uses a subcontractor, Contractor shall require such subcontractor to maintain the types and amounts of insurance that Contractor deems reasonable in light of the products and/or services to be provided by such subcontractor.

This Section is not intended to and is not to 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. **Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions) and MiDEAL members. Administrative fee payments must be made by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee.

   Checks can be mailed to:
   DTMB Cashiering
   P.O. Box 30681
   Lansing, MI 48909

   Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

   The administrative fee is due 45 calendar days from the last day of each calendar quarter and the purchasing activity report is due within 30 calendar days from the last day of each calendar quarter. For consistency quarters shall be considered to end the last day of March, June, September, and December of each calendar year.

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.

10. **Subcontracting.** Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any third party to act as a Fulfillment Partner or Hosting Provider (as defined in the attached SCHEDULE A – DATA SECURITY Schedule below) under this Contract. Contractor's engagement of any subcontractor, including Fulfillment Partners and Hosting Providers approved by the State, does not relieve Contractor of its representations, warranties, or obligations under this Contract. Without limiting the foregoing, Contractor will be responsible and liable for the acts and omissions of each subcontractor (including such subcontractor's employees who, to the extent providing Contract Activities, shall be deemed Contractor's employees) to the same extent as if such acts or omissions were by Contractor or its employees. Contractor must be the sole point of contact regarding all contractual matters, including payment and charges for all Contract Activities; 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; and Contractor will notify the State of the location of each subcontractor and indicate if it is located within the continental United States.

11. **Contractor Personnel. "Contractor Personnel**" means all employees of Contractor, or any subcontractors involved in the performance of Services hereunder. The State's Contract Administrator may require Contractor to remove or reassign Contractor Personnel by providing a notice to Contractor.
    a. Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.
    b. Prior to any Contractor Personnel performing any Services, Contractor will:

i. ensure that such Contractor Personnel have the legal right to work in the United States;

ii. upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract.

c. The State reserves the right to approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Contractor Personnel assigned to perform services under a Statement of Work.

d. **Acceptable Use Policy.** To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

12. Background Checks. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018. 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 and provide all necessary documentation and signatures. Notwithstanding the foregoing, Contractor may, without the State's prior approval, assign its right to receive payments due under the Contract to Fulfillment Partners approved by the State; provided that:

a. In addition to any other applicable terms under this Contract, all payment terms apply to payments made to Fulfillment Partners;

b. the Contractor remains responsible for its obligations hereunder, including but not limited to the complete fulfillment of any orders and resolution of any issues associated with an order;

c. For each payment assigned to a Fulfillment Partner, Cisco waives any claims and rights against the State that it now has or may have in the future in connection with the payment;

d. All payments and reimbursements made by the State to the Fulfillment Partner, shall be considered to have discharged those portions of the State's obligations under the Contract; and

e. Contractor agrees that the State is not obligated to pay or reimburse it for, or otherwise give effect to, any costs, taxes, or other expenses, or any related increases, directly or indirectly arising out of or resulting from the assignment of payment to its Fulfillment Partner, other than those that the State, in the absence of the assignment, would have been obligated to pay or reimburse under the terms of the Contract.

14. Change of Control. Contractor will notify within 30 days of any public announcement or otherwise once legally permitted to do so, 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 a SIGMA ordering document.

16. **Acceptance.** Contract Activities are subject to inspection and testing by the State within 15 calendar days of the State's receipt of them ("**State Review Period**"), unless otherwise provided in a Statement of Work (as defined in the Master Agreement). 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 30 calendar 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. **Delivery.** Contractor must deliver all Contract Activities F.O.B. destination, within the State premises with transportation and handling charges paid by Contractor, unless otherwise specified in a Statement of Work. All containers and packaging become the State's exclusive property upon acceptance.

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 30 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.**
    a. The warranty for hardware Products sold under this Contract is Contractor's standard limited warranty as set forth in Section 18a of the Master Agreement.
    b. The warranty for Services sold pursuant to Attachment 4 – Additional Contractor Terms and Conditions under this Contract is the following: a) Services will be performed in a workmanlike manner; b) where applicable, will materially comply with the applicable Service Description; and c) where applicable, will function in compliance with all requirements specified in a Statement of Work. The State must promptly notify Contractor of a breach of this warranty for Services and the State's sole and exclusive remedy for any breach of this warranty shall be, at the State's sole option, (i) reperformance of the services or (ii) termination of the applicable service, and return of the fees paid to Contractor by the State for such non-conforming services.
    c. For Software, Contractor represents and warrants to the State that:
        i. neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time: 1) conflict with or violate any applicable law; 2) require the consent, approval, or authorization of any governmental or regulatory authority or other third party; or 3) require the provision of any payment or other consideration to any third party other than payments to authorized Fulfillment Partners as contemplated under this Agreement;
        ii. when used by the State or any Authorized User (as defined in Attachment 3) in accordance with this Contract and the Documentation, the Software as delivered or installed by Contractor does not or will not fail to comply with any applicable law;
        iii. as provided by Contractor, the Software and Contract Activities do not and will not at any time during the Term contain any: 1) Harmful Code, when delivered or made available by the Contractor; or 2) Third party or Open-Source Components other than those specifically described in the Software's product documentation or as published by Cisco on its portal for Open-Source Components at https://www.cisco.com/go/opensource;
        iv. when used in accordance with the applicable documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with the applicable documentation;
        v. Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third-party software provider for any reason whatsoever;
        vi. no maintenance release or new version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software;

vii. To the best of its knowledge, Contractor will not advertise unrelated third-party products or services through the Cloud Software (whether with adware, banners, buttons, or other forms of online advertising) or link to external unrelated third-party web sites that are unrelated to the provision of the Cloud Software, unless otherwise identified in the product documentation. Notwithstanding the foregoing, unless otherwise prohibited by law, rule, regulation, or order, Contractor may (i) advertise its own products or services through the Cloud Software; or (ii) within the Cloud Software, advertise or link to third party applications or web sites for third party products that integrate with Contractor products.

viii. Software documentation and specifications are, and will be continually updated and maintained so that they continue to be, current, complete, and accurate and so that they do and will continue to fully describe the Software in all material respects such that at no time during the Term or any additional periods will the Software have any material undocumented feature; and

ix. during the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software, will apply solely to Contractor, and regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against state systems or networks.

20. Terms of Payment. Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 30 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in this Contract or an applicable Statement of Work. 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. All prices are exclusive 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 does not pay for overtime or travel expenses.

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. Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 20** or any dispute arising therefrom. 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. Any undisputed amounts not paid by the State when due for Contract Activities received may be assessed overdue account charges up to a maximum rate of 0.75% per month on the outstanding balance pursuant to 1984 PA 279, MCL 17.51, *et seq*.

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/SIGMAVSS 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. The State does not grant Contractor any security interest in any products purchased under this Contract.

21. RESERVED.

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 delivery order. The State will compensate Contractor for all work accepted under the Contract prior to issuance of the Stop Work Order. The State will not pay for the Contract Activities that were stopped under the stop work order, including but not limited to Contractor's lost profits 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 for amounts due to Contractor for Contract Activities accepted by the State on or before the date of termination and 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, destroy, or return to the State all materials, data (which includes without limitation State 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. Indemnification.

a. **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: any bodily injury, death, or damage to real or tangible personal property arising from the negligent or intentional acts or omissions of the Contractor or its officers, directors, employees, agents, successors and assigns of any of them.

b. **Intellectual Property Infringement Indemnity and Remedies.**

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 any third-party claim against the State that any of Contractor's Products or Software ("Cisco Technology") provided under the Contract infringes a third party's patent, copyright, or trademark, or other intellectual property right (the "IP Claim"). In addition, if an IP Claim is made , or if any Cisco Technology, or any component thereof, is found to be infringing or if any use of any Cisco Technology or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an IP claim, Contractor will either procure for the State the right to continue using the Cisco Technology or replace or modify the Cisco Technology with functionality that that has at least equivalent features and functionality. Only if Contractor determines that these alternatives are not reasonably available, Contractor may terminate the State's usage rights granted under this Contract upon written notice to the State and will refund to the State the pro-rated portion of any prepaid fees for Cisco Technology and/or services not provided or consumed and/or refund to the State the remaining net book value of the Cisco Technology calculated according to generally accepted accounting principles for the infringing Cisco Technology. Contractor agrees to reimburse the State for: (i) direct out-of-pocket expenses incurred in procuring a third-party solution to replace the relevant Cisco Technology (not including the purchase price of the replacement third party product or service); and (ii) direct out-of-pocket expenses incurred in the removal of the infringing Cisco Technology from the State's network and installation of the replacement third party solution in the State's network. Contractor's aggregate liability under (i) and (ii) in the preceding sentence will be limited to an amount equal to 110% of the net purchase price paid by the State for the infringing Cisco Technology subject to the claim. Contractor will have no liability to reimburse costs set out in (ii) unless such costs are reasonable and mutually agreed by the parties in advance.

Contractor has no obligation with respect to any IP Claim based on: (a) compliance with any designs, specifications, or requirements the State provides, or a third party provides on the State's behalf; (b) the State's modification of any Cisco Technology or modification by a third party on the State's behalf unless the modification was requested in writing by a

Contractor representative holding the position of Senior Vice President or higher and undertaken by the State in accordance with that request; (c) the State's failure to modify or replace Cisco Technology as required by Contractor, if such modification or replacement would have avoided the IP Claim; and (d) combination, operation, or use of Cisco Technology with non-Cisco products, software or business processes not approved in writing by the Contractor holding the position of Senior Vice President or higher, unless (1) the combination is of a type reasonably contemplated for such Cisco Technology; (2) the Product forms a material part of the invention subject to the Claim, and (3) the infringement could not be avoided by an alternative combination falling within the scope of Contractor's recommendation in the Documentation (a "Covered Combination"). For the exclusion covered under subsection (d) in the preceding sentence, Contractor shall only be responsible for its respective pro-rata share of calculable damages based on the value of Contractor's contribution into the Covered Combination relative to the total value of the Covered Combination (including, without limitation, the value contributed by other vendors or the State).

c. **Indemnification Procedure**. The foregoing indemnification obligations in Sections a and b above are conditioned upon the State promptly notifying the Contractor in writing of the claim, suit, or proceeding for which the Contractor is obligated under this Section (however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced), cooperating with, assisting, and providing information to, the Contractor as reasonably required, and granting the Contractor the right to defend or settle such claim, suit, or proceeding; provided that State has provided its written consent (not to be unreasonably withheld) and any such settlement or compromise includes a release of the State from all liability arising out of such claim, suit or proceeding. The State, at its own expense, may retain its own legal representation.

The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) at its own expense 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.

The State is constitutionally prohibited from indemnifying Contractor or any third parties.

This Section states the Contractor's entire obligation and the State's exclusive remedy along with any other remedies available under applicable law regarding any IP Claims against the State.

27. Limitation of Liability and Disclaimer of Damages.

a. Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS, REVENUE, ANTICIPATED SAVINGS, LOST BUSINESS OPPORTUNITIES, USE OF ANY PRODUCT OR SERVICE, OPPORTUNITY, GOODWILL OR REPUTATION.

b. Limitation of Liability. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE GREATER OF (I) THREE MILLION DOLLARS ($3,000,000.00) OR (II) THE MONEY PAID TO CONTRACTOR (INCLUDING FULFILLMENT PARTNERS) BY THE STATE UNDER THIS CONTRACT IN THE TWELVE (12) MONTH PERIOD PRIOR TO THE EVENT OR CIRCUMSTANCES THAT FIRST GAVE RISE TO SUCH LIABILITY.

c. Exceptions. Subsections (a) (Disclaimer of Damages) and (b) (Limitation of Liability) above shall not apply to:

i. Contractor's obligations under Section 26 of this Contract; and

ii. The parties agree that for claims related to Contractor's obligations under Section 29(d) of this Agreement, Contractor agrees to a per incident cap on liability of $5,000,000.00 (five million dollars). The cumulative aggregate cap on liability for all claims arising under Section 29(d) under this Agreement shall not exceed $15,000,000.00 (fifteen million dollars) during the term of the Agreement.

28. **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.

29. **State Data.**

a. Ownership. The State's data ("**State Data**") includes any data collected, used, processed, stored, or generated as the result of the Contract Activities, including but not limited to Customer Content, Systems Information, and Personal Data (as defined in the definitions section above). Personal Data includes without limitation, any information that identifies an individual, or personally identifiable information ("**PII**"), 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 personal health information ("**PHI**") as 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.

i. 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.

ii. Notwithstanding the foregoing, unless otherwise agreed to in writing, data that is categorized as Systems Information may be retained and used by Contractor in accordance with the applicable documentation for such Product or Service ("Contractor's Objectives") that the State has procured, and may be shared with Contractor's partners, distributors and contractors, including but not limited to Hosting Providers, Fulfillment Partners and other subcontractors under this Contract (collectively, "trusted ecosystem") for Contractor's Objectives, provided that, (a) prior to the State procuring Contractor's Products and Services, Contractor will, upon request, provide the State with Product-specific and/or Service-specific documentation, including data privacy sheets, specifying the Systems Information the Contractor collects and/or has access to (if any), how such information will be used, applicable data retention policies, and if and/or how the State can control Contractor's access to such information; (b) such documentation will not materially change during the Term; and (c) each participant in the trusted ecosystem has agreed contractually with Contractor to confidentiality, applicable law and other requirements that are consistent with Contractor's obligations to the State under this Contract. For the avoidance of doubt, all System Information licensed to Contractor under this subsection is "as is" without warranty of any kind and Contractor's use of such System Information shall be at Contractor's sole and exclusive risk, and the State will have no liability whatsoever in connection with Contractor's or any third party's use of such System Information.

iii. Contractor shall access, process and use Personal Data collected under this Contract in accordance with (a) applicable privacy and data protection laws; (b) Contractor's Personal Data – Data Brief attached hereto as Attachment 6 – Personal Data Brief; and (c) Contractor's applicable Product-specific and/or Service-specific Privacy Data Sheets (available at https://trustportal.cisco.com), provided that any changes to such data sheets shall not diminish Contractor's obligations to secure Personal Data and no such changes shall materially decrease the level of security afforded to the State's Personal Data. Moreover, Contractor shall: a) keep the State's Personal Data secure pursuant to the terms of the attached SCHEDULE A DATA SECURITY Schedule; b) keep such data confidential and only share such data with third parties engaged by Contractor that are identified in the Contractor's Product-specific and/or Service-specific documentation ("Sub-processors") who must have agreed contractually with Contractor to confidentiality, applicable law and other requirements that are consistent with Contractor's obligations to the State under this Contract, and only for the purposes specified in such documentation and/or the performance of this Contract; and c) in no event shall Contractor sell, rent, or lease the State's Personal Data. The terms in this paragraph do not apply to any Personal Data included within Customer Content. Personal Data included within Customer Content must be treated as Customer Content. If Contractor materially changes any of their Product-specific and/or Service-specific documentation as it pertains to privacy, data collection, or use, then the State must immediately provide Contractor with its intent to terminate for such reasons and a 30-day cure period within which Contractor may cure such material change. If Contractor is unable to cure within the aforementioned cure period, the State has the right to terminate the applicable product or service without liability or penalty, including without limitation, payment of early termination or other fees, and Contractor shall refund any prepaid amounts for the applicable product

or service prorated to the date of such termination. Upon such termination, Contractor's rights to access, process and use such Personal Data will immediately and automatically terminate and State agrees to pay for amounts due to Contractor for Contract Activities accepted and/or consumed by the State up until the point of such termination.

iv. If the State, in its sole discretion determines that Contractor's access, processing, or use of State Data as described in this Section would cause the State to be in violation of any law, rule, regulation, or order, then the State has the right to terminate the applicable product or service without liability or penalty, including without limitation, payment of early termination or other fees, and Contractor shall refund any prepaid amounts for the applicable product or service prorated to the date of such termination. Upon such termination, Contractor's rights to access, process and use of such State Data will immediately and automatically terminate and State agrees to pay for amounts due to Contractor for Contract Activities accepted and/or consumed by the State up until the point of such termination.

c. RESERVED.

d. Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or poses an imminent threat of compromising the security, confidentiality, availability, or integrity of State Data that references the State ("Data Breach"), Contractor must, as applicable: (a) notify the State without undue delay after becoming aware of a Data Breach, but no later than twenty-four (24) hours after confirmation of a Data Breach; (b) reasonably cooperate with the State in investigating the occurrence, including making available, to the extent possible, relevant records and other materials required to comply with applicable law or as otherwise reasonably required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) except as required in order to comply with applicable law, with approval and assistance from the State, 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; (ii) subject to the limitation of liability set forth in this Agreement under Section 27(c)(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 12 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) subject to the limitation of liability set forth in this Agreement under Section 27(c)(ii), pay for the reasonable and actual costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) subject to the limitation of liability set forth in this Agreement under Section 27(c)(ii) 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 incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (h) be responsible for restoring lost State Data up to the backup provided by the State or if Contractor committed to performing backups as identified in product/service documentation then Contractor will restore to the backup as provided for in the product/service documentation; and (i) provide to the State a detailed plan within a mutually agreed upon timeframe 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, not be tangentially used for any solicitation purposes, 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. Except as required to comply with applicable law, the State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, referencing or identifying the State must be reviewed and approved by the State in writing prior to its dissemination. The parties agree that the costs described in sub-sections (c)(ii), (d), (f), and (h) relating to a breach of this **Section 29** are to be considered direct damages and not consequential damages. This Section survives termination or expiration of this Contract.

30. 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). Except for De-Identified Systems Information, all 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 or necessary for Contractor's delivery of products and services to the State; (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 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 any unauthorized use or disclosure of any Confidential Information by the other party. 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. Discovery. To the extent permitted by law, each party shall notify the other party upon receipt of any requests seeking access to the Confidential Information described in this Section 30 promptly upon receipt of notice of the request for disclosure. A party will be authorized to disclose Confidential Information as may be required by applicable law pursuant to a valid order issued by a court or government agency or relevant regulatory authority (including a stock exchange), or a FOIA request, provided that the party provides, to the extent permitted by law: (i) prior written notice to the other party of such obligation; and (ii) the opportunity to oppose such disclosure. The notice and opportunity to oppose disclosure requirements do not apply to requests received by the State under the FOIA.

e. 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.

f. 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 30 calendar days (or other timeframe mutually agreed to in writing) from the date of termination, return to the other party upon request or make available for at least 30 calendar days for the State to download 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. After complying with the foregoing, Contractor must permanently sanitize or destroy the Confidential Information from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitation methods or as otherwise agreed by the parties. Upon request, each party must certify the destruction of the other party's Confidential Information in writing to the other party within thirty (30) days of the other party's request for destruction.

However, each party's legal ability to destroy the other party's Confidential Information may be restricted by its retention and disposal schedule, in which case the other party's Confidential Information will be destroyed after the retention period expires. Additionally, each party may retain the other party's Business Contact Information to the extent permitted by law in order to manage the commercial relationship between the parties.

31. Data Privacy, Information Security, Backup, and Disaster Recovery.

i. **Data Privacy and Information Security**. Throughout the Term and at all times in connection with its actual or required performance of the Contract Activities, Contractor will maintain and enforce an information security program that complies with the requirements of the State's data security policies as set forth in the attached **Schedule A** – Data Security Schedule

ii. **Third Party Components**. Throughout the Term, Contractor will make available updated information identifying and describing any third party and Open-Source Components included in the Software.

iii. **Data Storage, Backup, Restoration and Disaster Recovery**. For State Data that is within Contractor's possession or control, Contractor must maintain or cause to be maintained backup, redundancy, and disaster avoidance and recovery procedures designed to safeguard State Data and the State's other Confidential Information, including Contractor's processing capability and the availability of the Software, in each case throughout the Term and at all times in connection with its actual or required performance of the Contract Activities hereunder. Contractor shall make available to the State information to enable the State to procure products and services covered by this Contract that allow for all State Data backed up by Contractor to be located in the continental United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section**.**

1. Data Storage. Contractor will provide sufficient storage capacity pursuant to the terms of the licensed product.

2. Data Backup. If and as agreed by the parties, Contractor will conduct, or cause to be conducted, periodic back-ups of State Data and perform, or cause to be performed, other periodic offline back-ups of State Data and store and retain such back-ups as specified in a Statement of Work, applicable Order, applicable product documentation, or otherwise agreed in writing by the parties. Contractor shall provide the State with information to enable the State to procure services that include the ability to extract State Data in Contractor's possession in a format and within a timeframe identified in the product/service documentation or as mutually agreed to by the parties.

3. Data Restoration. If the data restoration is required due solely to the actions or inactions of the Contractor or its subcontractors, Contractor will promptly notify the State and complete actions required to restore service to normal production operation at its sole cost and expense. If requested, Contractor will restore data from Contractor's last uncorrupted backup of State Data upon written notice from the State and within a timeframe that is mutually agreed upon by the parties, and will be responsible for restoring lost State Data up to the backup provided by the State or if Contractor committed to performing backups as identified in product/service documentation then Contractor will restore to the backup as provided for in the product/service documentation.

4. Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO), and a Recovery Time Objective (RTO) as required by the State in the applicable Statement of Work, Order, or otherwise agreed in writing by the parties (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of Cloud Software. Upon request, Contractor shall make available to the State a subject matter expert to meet virtually and provide information on Contractor's DR Plan and tests, only to the extent that providing such information does not jeopardize Contractor's security posture. Contractor will actively test, review, and update the DR Plan on at least an annual basis using industry best practices as guidance.

32. RESERVED.

33. RESERVED.

34. 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.

35. 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) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (d) the Contract Activities are merchantable and fit for the specific purposes identified in the Contract; (e the Contract signatory has

the authority to enter into this Contract; (f) 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; (g) 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; and that (h) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606. 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 forCause.

36. 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.

37. Compliance with Laws. Contractor must comply with all federal, state, and local laws, rules, and regulations.

38. RESERVED.

39. RESERVED.

40. Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq*., and Executive Directive 2019-09. 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 (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. 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 of the foregoing, a "Force Majeure Event"). 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. No Force Majeure Event modifies or excuses Contractor's obligations under **Sections 29** (State Data), **30** (Non-Disclosure of Confidential Information), or **26** (Indemnification), or any Disaster Recovery, data backup or restoration, data retention, or security requirements under the Contract.

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. RESERVED.

49. RESERVED.

50. 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.

51. Waiver. Failure to enforce any provision of this Contract will not constitute a waiver.

52. 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.

53. Contract Modification. This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

54. Accessibility Requirements.

a. Contractor adopts the WCAG 2.0 Level A and AA standards as best practices for the design and testing of its Software products provided under the Contract. Contractor's objective is to deliver WCAG 2.1 Level A and where possible AA compliance over the 18 months after the execution date of this Contract.

b. Contractor maintains PATs for substantially all of the Software products provided under the Contract., currently located at https://www.cisco.com/c/en/us/about/accessibility/voluntary-product-accessibility-templates.html. In the event the State identifies a Software product for which Contractor has not prepared a PAT, Contractor will prioritize and expedite the preparation of a PAT for that Software product.

c. Throughout the Term of the Contract, at no additional costs to the State, Contractor must:

   i. ensure that products and offers it provides to the state, including any upgrades or modifications to those products and offers, meet, or exceed (a) applicable legal requirements, and (b) any WCAG or other conformance claims Contractor makes in its applicable PAT(s) and/or other written material related to accessibility that are applicable to those products and offers;

   ii. promptly respond to and resolve any complaint the State receives demonstrating that Contractor's products and offers do not meet or exceed (a) applicable legal requirements, and (b) any WCAG or other conformance claims Contractor makes in its applicable PAT(s) and/or other written material related to accessibility that are applicable to those products and offers, but only to the extent resolving any such complaint is commercially reasonable (e,g., no obligation to resolve complaints for a product slated for imminent "end of life"); and

   iii. participate in the State of Michigan Digital Standards Review described below.

d. State of Michigan Digital Standards Review. The State may conduct a Digital Standards Review to assess accessibility and compliance with legal requirements applicable to Contractor's Software products and WCAG 2.0 Level AA. Contractor must reasonably assist the State with such review, which requires Contractor to submit evidence to the State to validate that its products meet or exceed (a) applicable legal requirements, and (b) any WCAG or other conformance claims Contractor makes in its applicable PAT(s) and/or other written material related to accessibility that are applicable to those products and offers. Subject to the limitations identified in Section 54(c)(ii), Contractor must promptly resolve any finding that its products do not meet or exceed (a) applicable legal requirements, and (b) any WCAG or other conformance claims Contractor makes in its applicable PAT(s) and/or other written material related to accessibility that are applicable to those products and offers, at its sole cost and expense.

e. Failure to comply with the requirements in this **Section** shall constitute a material breach of this Contract. Contractor shall be provided with a sixty (60) day cure period within which to cure any such breaches.

55. CJIS Compliance. Contractor must comply with the following if CJIS data security requirements are applicable:

a. Contractor will comply with all Criminal Justice Information Services (CJIS) Security Policy requirements that are communicated to the Contractor in writing, including but not limited to the Federal Bureau of Investigation (FBI) CJIS Security Addendum attached as Exhibit B to the attached SCHEDULE A– DATA SECURITY Schedule and executing any additional agreement(s) if necessary and applicable.
b. The State reserves the right to perform additional background checks on Contractor Personnel as may be required to comply with the CJIS Security Policy.
c. During the term, Contractor will maintain complete and accurate records relating to its data protection practices and the security of any of the State's Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State's Confidential Information and any other information relevant to its compliance with this Section. Contractor shall make all such records, appropriate personnel, and relevant materials available in the event of an audit initiated by the State or the FBI.

56. HIPAA Compliance. Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if applicable.

SCHEDULE A – DATA SECURITY Schedule

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Participating Addendum, Attachment 1 – State of Michigan Terms and Conditions, or Master Agreement.

"**Contractor Security Officer**" has the meaning set forth in **Section 2** of this Schedule.

"**FedRAMP**" means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

"**FISMA**" means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.).

"Hosted Services" means Contractor's hosting, management and operation of any operating environment, Software, other services (including support and subcontracted services), and related resources for access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

"Hosting Provider" means any subcontractor that is providing any or all of the Hosted Services under this Contract.

"**NIST**" means the National Institute of Standards and Technology.

"**PCI**" means the Payment Card Industry.

"**PSP**" or **"PSPs"** means the State's IT Policies, Standards and Procedures.

"**SSAE**" means Statement on Standards for Attestation Engagements.

"**Security Accreditation Process**" has the meaning set forth in **Section 6** of this Schedule.

"**Services**" means Contract Activities.

2. Security Officer. Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**").

3. Contractor Responsibilities. 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 any State Data in Contractor's or its subcontractor's possession; and

(e) ensure that all Contractor Personnel comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. Contractor's FedRAMP offerings must at all times materially comply with NIST 800-53 moderate controls.

This responsibility also extends to all service providers and subcontractors of FedRAMP offerings with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. Acceptable Use Policy. To the extent that Contractor Personnel has been granted an account with user access rights to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All such Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

5. Protection of State's Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

5.1 for Contractor Products selected by the State that are identified as FedRAMP authorized and the Hosted Services are provided by one or more Hosting Providers, each Hosting Provider must maintain FedRAMP authorization for the Products' Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may immediately terminate its use of Contractor's Products for cause pursuant to **Section 23** of the Contract;

5.2 for Contractor Products where the Hosted Services are provided by the Contractor, the Contractor will provide the State with information to enable the State to procure Contractor's Products. Products that maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs ("**State Compliant SSAE 18 Audit**").

5.3 for Contractor Products selected by the State that are FedRAMP authorized or meet State Compliant SSAE 18 Audit requirements and where the Hosted Services are provided by the Contractor, Contractor will maintain either a FedRAMP authorization or a State Compliant SSAE 18 Audit throughout the Term. If the State selects such Products and the Contractor fails to maintain a FedRAMP authorization or State Compliant SSAE 18 Audit throughout the Term, the State, at its sole discretion, may immediately terminate its use of the Contractor Products for cause pursuant to **Section 23** of the Contract.

5.4 provide the State with information to enable the State to procure Contractor's Services and Products that ensure that the Software and State Data is securely hosted, supported, administered, accessed, and backed up in a data center(s) that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

5.5 provide the State with information to enable the State to procure Contractor's Services and Products that maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its processing of the State Data that complies with the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.6 provide technical and organizational safeguards against accidental, unlawful, or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data;

5.7 take all reasonable measures designed to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "malicious actors" and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) State Data from being commingled with or contaminated by the data of other customers or their users of the Services, the foregoing does not prevent Contractor from aggregating Systems Information as authorized under this Contract; and (iii) unauthorized access to any of the State Data;

5.8 ensure that Customer Content is encrypted in transit and at rest using industry best practices, and provide the State with information to enable the State to procure Services that encrypt State Data, in transit and at rest, using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.9 provide the State with information to enable the State to procure Services and Products that ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;

5.10 provide the State with information to enable the State to procure Services or Products that ensure the Hosted Services or Products implement NIST compliant multi-factor authentication for privileged/administrative and other identified access.

6. Security Accreditation Process. Throughout the Term, Contractor will reasonably assist the State, at no additional cost, with its **Security Accreditation Process**, which refers to the annual completion, upon request, of an industry standard security questionnaire such as a SIG or CAIQ and collaborate with the State in good faith to achieve resolution of unresolved SSP control questions for Contractor Products selected by the State that are FedRAMP authorized.

7. Unauthorized Access. Contractor may not access, and shall not permit any access to, State systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Notwithstanding the foregoing, for remote technical support / troubleshooting services requested by the State's users, the requirement of express prior written authorization shall be replaced with the authorization and access granted by the State's user during Contractor's provision of such remote technical support / troubleshooting service. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's or it's users' authorization pursuant to this Section. All authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

8. Security Audits.

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the relevant security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 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 Services and from time to time during the term of this Contract but not more often than once per calendar year. 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. The parties shall agree on the specific time, location, duration, manner, and scope of such audit. If the State chooses to perform an on-site audit, Contractor will make relevant records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least 6 weeks prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except in the case of a material data breach impacting State Data; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract.

8.3 During the Term, Contractor will, when requested by the State, provide a redacted copy or summary of Contractor's or Hosting Provider's FedRAMP System Security Plan(s) for the FedRAMP Services purchased by the State to the extent permitted by law, or make available from Contractor's online resources (ex: Cisco's Trust Portal) to the State SOC 2 Type 2 report(s) that the Contractor maintains if identified in the product/service documentation. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 With respect to State Data, Contractor must resolve any material audit findings for Contractor Products selected by the State that do not meet applicable regulatory controls as identified in Contractor's product documentation and/or other written material applicable to such Products made available to the State as of the date of procurement of such Product or Service.

8.5 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work or its use of the Contractor Services or Products without limitation and without liability if the State determines that Contractor materially fails or has failed to meet its obligations under this **Section 8** and has not cured such failure within 60 days.

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate, and validate all vulnerabilities identified by the scans pursuant to the Contractor'sprioritization of such vulnerabilities, based upon their criticality (e.g., nature, severity, likelihood).

Upon request, Contractor shall provide the State with information to enable the State to procure only Contractor Services and Products that perform application scanning and remediation that include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST).

9.2 Static Application Security Testing (SAST) - Scanning source code for software and applications provided to the state for vulnerabilities, analysis, remediation, and validation.

9.3 Software Composition Analysis (SCA) – Third party and/or Open-Source Scanning for vulnerabilities, analysis,remediation, and validation.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programing interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must provide the State with information to enable the State to procure Services that ensure the infrastructure and applications are scanned using a PCI approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly. Contractor will address the remediation of issues identified in the scan according to the Contractor's prioritization of such issues, based upon their criticality (e.g., nature, severity, likelihood).

11. Nonexclusive Remedy for Security Breach.

11.1 Any material failure of the Services to substantially meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, after providing the Contractor with a 60 day cure period, at its option, may terminate the Contract immediately upon written notice to Contractor, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE A, Exhibits:

Contractor must comply with the following Exhibits when applicable:

Exhibit A – Tax Regulation (Federal and State)
Exhibit B – FBI CJIS
Exhibit C - PCI Compliance and CEPAS

SCHEDULE A, Exhibit A – Federal Tax Regulation
(Commonly known as IRS Publication 1075, Exhibit 7)

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.
(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
(3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.
(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
(6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
(7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
(8) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access

FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

SCHEDULE A, Exhibit A – State of Michigan, State Tax Information Attachment

SAFEGUARD REQUIREMENTS OF CONFIDENTIAL TAX DATA

This section 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 l941 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 subcontractorswill 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 contract 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 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 State identified and approved methods for remote vendor access are as follows:

- SecureID through VPN – State 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 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.

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:

1. 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.

   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.

2. 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 sub-contractor. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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, destroy paper using crosscut shredders which produce particles that are 1 mm x 5mm (0.04in x 0.2 in.) in size (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.

XI. Security Breach Notification

The Contractor is required 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 misuse or disclosure. The Contractor may substitute its internal form for Form 4000 if all pertinent information is included.

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

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

XIII. Certification of Compliance

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 contract 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 Contractor, the Contractor agrees to provide full cooperation to conduct a thorough security review. The review will validate compliancy with the Contract, 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.

Reset Form

Michigan Department of Treasury
3337 (Rev. 10-16)

Vendor, Contractor or Subcontractor Confidentiality Agreement

The Revenue Act, Public Act 122 of 1941, MCL 205.28(1)(f), the City Income Tax Act, Public Act 284 of 1964, MCL 141.674(1), and Internal Revenue Code (IRC) 6103(d), make all information acquired in administering taxes confidential. The Acts and IRC hold 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 Acts and IRC. 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 RR#, 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 disclose or 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).

City Penalties
MCL 141.674(2) provides that any person divulging confidential City Tax information is guilty of a misdemeanor and subject to a fine not exceeding $500 or imprisonment for a period not exceeding 90 days, or both, for each offense.

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

Michigan Department of Treasury
4000 (Rev. 05-14)

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?

☐ Treasury ☐ Federal Tax Information ☐ Other State Agency, specify _____ ☐ Other _____

Incident Category (select all that apply)

☐ Passwords Shared/Stolen	☐ Computer Virus/Spam	☐ Paper Archives Compromised
☐ Misrouted Communications	☐ Data Destruction/Deletion	☐ Safe/Lockbox/other Compromise
☐ Unauthorized Access	☐ Backups Missing or Stolen	☐ Delivery of Documents Lost
☐ Fraudulent Actions	☐ Hacking of Networks/Systems	☐ Inappropriate Destruction Paper
☐ Lost/Stolen Information/Data	☐ Improperly Secured Sys/Web	☐ Inappropriate Destruction Media
☐ Lost/Stolen Cash/Checks	☐ Circumvention of Security Protocols	☐ Lost/Stolen Equipment
☐ Inappropriate Building Access	☐ _____	☐ _____

Incident Affects

☐ Financial Information/Resources ☐ Personal Information (SSN, Driver License No. Financial information) ☐ Unauthorized/Unlawful Activity

☐ Confidential/Sensitive Information ☐ Human Resources (threat) ☐ 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)? ☐ Yes ☐ 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?	How many notifications were sent?	Breach Notification Method?
☐ Yes ☐ No		☐ E-mail ☐ Telephone ☐ US Mail ☐ Web

Who was notified?	Date notification was issued

Incident Cost

☐ Check if incident costs are less than $250. If $250 or more, complete the detailed summary of costs below.

Manhours:

Treasury $_____

DTMB-OES $_____

DTMB-Treasury Agency Services $_____

Other:

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's Telephone Number

Preparer Signature	Date

OFFICE OF PRIVACY AND SECURITY USE ONLY

Administrator, Office of Privacy and Security Signature	Date

SCHEDULE A, Exhibit B - FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks, and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

1.03 Responsibilities of the Contracting Government Agency.

2.00 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI willprovide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA andContractor. Upon termination, the Contractor's records containing CHRI must be deleted orreturned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating, or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating, or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

SCHEDULE A, Exhibit C – PCI Compliance and CEPAS

PCI Compliance.
Contractors that process, transmit store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.
The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g., Visa, MasterCard, and Discover) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third-party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance (AOC) or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

CEPAS Electronic Receipt Processing Standard.
All electronic commerce applications that allow for electronic receipt of credit or debit card and electronic check transactions must be processed via the State's Centralized Electronic Payment Authorization System (CEPAS). To minimize the risk to the State, full credit/debit card numbers, sensitive authentication data, and full bank account information must never be stored on state-owned IT resources.

Federal Provisions Addendum

This addendum applies to purchases that will be paid for in whole or in part with funds obtained from the federal government. The provisions below are required, and the language is not negotiable. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to the State's Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. Equal Employment Opportunity

If this Contract is a "**federally assisted construction contract**" as defined in 41 CFR Part 60-1.3, and except as otherwise may be provided under 41 CFR Part 60, then during performance of this Contract, the Contractor agrees as follows:

(1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

(4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in

Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: *Provided*, that if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

2. Davis-Bacon Act (Prevailing Wage)

If this Contract is a **prime construction contracts** in excess of $2,000, the Contractor (and its Subcontractors) must comply with the Davis-Bacon Act (40 USC 3141-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"), and during performance of this Contract the Contractor agrees as follows:

(1) All transactions regarding this contract shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29C.F.R. pt. 5 as may be applicable. The contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable.

(2) Contractors are required to pay wages to laborers and mechanics at a rate not less than theprevailing wages specified in a wage determination made by the Secretary of Labor.

(3) Additionally, contractors are required to pay wages not less than once a week.

3. Copeland "Anti-Kickback" Act

If this Contract is a contract for construction or repair work in excess of $2,000 where the Davis-Bacon Act applies, the Contractor must comply with the Copeland "Anti-Kickback" Act (40 USC 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"), which prohibits the Contractor and subrecipients from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled, and during performance of this Contract the Contractor agrees as follows:

(1) Contractor. The Contractor shall comply with 18 U.S.C. §874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this contract.

(2) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA or the applicable federal awarding agency may by appropriate instructions require, and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.

(3) Breach. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a Contractor and Subcontractor as provided in 29 C.F.R. § 5.12.

4. Contract Work Hours and Safety Standards Act

If the Contract is **in excess of $100,000** and **involves the employment of mechanics or laborers**, the Contractor must comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5), as applicable, and during performance of this Contract the Contractor agrees as follows:

(1) Overtime requirements. No Contractor or Subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (1) of this section the Contractor and any Subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such Contractor and Subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (1) of this section, in the sum of $27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.

(3) Withholding for unpaid wages and liquidated damages. The State shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the Contractor or Subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.

(4) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clauses set forth in paragraph (1) through (4) of this section and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.

5. Rights to Inventions Made Under a Contract or Agreement

If the Contract is funded by a federal "funding agreement" as defined under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

6. Clean Air Act and the Federal Water Pollution Control Act

If this Contract is **in excess of $150,000,** the Contractor must comply with all applicable standards, orders, and regulations issued under the Clean Air Act (42 USC 7401-7671q) and the Federal Water Pollution Control Act (33 USC 1251-1387), and during performance of this Contract the Contractor agrees as follows:

Clean Air Act

1. The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
2. The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.
3. The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

Federal Water Pollution Control Act

1. The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
2. The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.
3. The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

7. Debarment and Suspension

A "contract award" (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (51 FR 6370; February 21, 1986) and 12689 (54 FR 34131; August 18, 1989), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

(1) This Contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the Contractor is required to verify that none of the Contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) The Contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) This certification is a material representation of fact relied upon by the State. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

(4) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

8. Byrd Anti-Lobbying Amendment

Contractors who apply or bid for an award of **$100,000 or more** shall file the required certification in Exhibit 1 – Byrd Anti-Lobbying Certification below. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

9. Procurement of Recovered Materials

Under 2 CFR 200.322, Contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.

(1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—

a. Competitively within a timeframe providing for compliance with the contract performance schedule;

b. Meeting contract performance requirements; or

c. At a reasonable price.

(2) Information about this requirement, along with the list of EPA- designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive- procurement-guideline-cpg-program.

(3) The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

10. Additional FEMA Contract Provisions.

The following provisions apply to purchases that will be paid for in whole or in part with funds obtained from the Federal Emergency Management Agency (FEMA):

(1) Access to Records. The following access to records requirements apply to this contract:

a. The Contractor agrees to provide the State, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

b. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

c. The Contractor agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the contract.

d. In compliance with the Disaster Recovery Act of 2018, the State and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

(2) Changes.

See the provisions regarding modifications or change notice in the Contract Terms.

(3) DHS Seal, Logo, And Flags

The Contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

(4) Compliance with Federal Law, Regulations, and Executive Orders

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the contract. The Contractor will comply with all applicable Federal law, regulations, executive orders, FEMA policies, procedures, and directives.

(5) No Obligation by Federal Government

The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the State, Contractor, or any other party pertaining to any matter resulting from the Contract.

(6) Program Fraud and False or Fraudulent Statements or Related Acts

The Contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor's actions pertaining to this contract.

Exhibit 1 - Byrd Anti-Lobbying Certification

Contractor must complete this certification if the purchase will be paid for in whole or in part with funds obtained from the federal government and the purchase is greater than $100,000.

APPENDIX A, 44 C.F.R. PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The Contractor, Cisco Systems, Inc., certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.

E-SIGNED by Jenn Pate
on 2021-08-12 13:07:47 EDT

Signature of Contractor’s Authorized Official

Jenn Pate Legal Analyst

Name and Title of Contractor’s Authorized Official

2021-08-12 13:07:47 UTC

Date

Attachment 2
State of Michigan
IT Asset Management (ITAM) Requirements

ASSET REPORTING

Contractor must ensure all Fulfillment Partners provide the following reports:

- **Shipping Report – Weekly (when there is a shipment)**
- **Purchase Report – Quarterly**

Weekly Shipping Report

a. The Fulfillment Partner must provide a weekly shipping report directly to the State of the items shipped to Depot, or to any State of Michigan Facility, once a Delivery Order/Purchase Order is received by a Fulfillment Partner.

b. This report must be in Excel format and sent to the State as directed by the Contract Administrator. The format should stay the same unless agreed to by the Contractor and DTMB.

c. The required fields are shown below:

Column Name	Description
Ship to	e.g., General Services Building, Lake Michigan Hosting Center, Lake Superior Hosting Center, Hannah Building, etc. This would be a field with a provided drop down menu
Address	The street address where the product was delivered
Tracking Number	The shipping company's tracking #
ServiceTag	This is manufacturer serial #
State PO	The Purchase Order number issued by the state
Agency	The Agency Name from the list below: Attorney General Department of Community Health Department of Environmental Quality Department of Human Services

	Department of Human and Health Services Department of Insurance and Financial Services Department of Technology, Management and Budget - IT Department of Technology, Management and Budget - MB Department of Military & Veterans Affairs Department of Natural Resources Governor's Office Department of Licensing and Regulatory Affairs Civil Service Commission Department of Agriculture and Rural Development Department of Civil Rights Department of Education Department of Corrections Department of State Department of Transportation Michigan State Police Department of Talent and Economic Development Department of Treasury
Category	Limited to one of the following: Workstation Monitor Printer Peripheral Network Hardware Router Switch Server Storage Phone Radio Software Other
Model	Manufacturer Model
Qty	Quantity purchased
Price	The price per item
ShipDate	The date the equipment is shipped
Mfg Part #	The manufacturer part number
Cust PO #	The vendor's internal PO when ordering from other suppliers
Shipment Carrier	e.g. UPS, FedEx, etc.
Agency Code	Agency Code table: 111 Attorney General

	391 Department of Community Health 761 Department of Environmental Quality 431 Department of Human Services 491 Department of Human and Health Services 651 Department of Insurance and Financial Services 084 Department of Technology, Management and Budget - IT 071 Department of Technology, Management and Budget - MB 511 Department of Military & Veterans Affairs 751 Department of Natural Resources 011 Governor's Office 641 Department of Licensing and Regulatory Affairs 191 Civil Service Commission 791 Department of Agriculture and Rural Development 151 Department of Civil Rights 313 Department of Education 472 Department of Corrections 231 Department of State 591 Department of Transportation 551 Michigan State Police 186 Department of Talent and Economic Development 271 Department of Treasury
Order Number	The vendor internal order number that matches the internal order number printed on the packing slip
Expected Delivery Date	The date the equipment expected to deliver
Warranty Tag	(Optional) The tag number used for warranty services (could be the same as the serial number)
Reporting Vendor	Vendor who provided this purchase report
Manufacturer Name	The name of the company that manufactures the product

Quarterly Purchase Report

a. The Fulfillment Partner must provide a quarterly purchase report of items shipped to the State of Michigan.

b. This report must be in Excel format and sent to the State as directed by the Contract Administrator.

c. The reports must detail the information below on an individual PO line item basis. Each asset with serial numbers to be listed on individual lines of the reports.

Column Name	Description
Client PO Number	The purchase order number issued by the state

PO Agency Code	Code Agency Name --- -------- 111 Attorney General 391 Department of Community Health 761 Department of Environmental Quality 431 Department of Human Services 491 Department of Human and Health Services 651 Department of Insurance and Financial Services 084 Department of Technology, Management and Budget - IT 071 Department of Technology, Management and Budget - MB 511 Department of Military & Veterans Affairs 751 Department of Natural Resources 011 Governor's Office 641 Department of Licensing and Regulatory Affairs 191 Civil Service Commission 791 Department of Agriculture and Rural Development 151 Department of Civil Rights 313 Department of Education 472 Department of Corrections 231 Department of State 591 Department of Transportation 551 Michigan State Police 186 Department of Talent and Economic Development 271 Department of Treasury
PO Department	The Agency Name from the list above
Address	The street address where the product was delivered
City	The city where the product was delivered
Zip	The zip code where the product was delivered
Manufacturer Name	The name of the company that manufactures the product
MFG P/N	The manufacturer's part number
Category	Limited to one of the following Workstation Monitor Printer Peripheral Network Hardware Router Switch Server Storage Phone Radio Software Other

Model/Description	The description of the product
Qty	The quantity purchased
Unit Invoice Price	The price of one of these items
Extended Invoice Price	The total price of all the items. Qty x Unit price
Vendor Invoice Date	The date of the invoice
Vendor Invoice Number	The number of the invoice
Ship Date	The date the product was shipped
Shipper	The name of the shipping company
Tracking Number	The shipping company's tracking number
Delivery Date	The date the product was delivered
Warranty End Date	The date that the warranty ends
Vendor Order Number	(Optional) The vendors order number
Serial Number	The serial number of the product. Each item that has a serial number must be on a separate line.
Reporting Vendor	Vendor who provided this purchase report

Attachment 3 – Software License Terms and Conditions

The parties agree that this Attachment 3 – Software License Terms and Conditions modifies and replaces Attachment A, Exhibit 1 – Additional Contractor Terms and Conditions, included in the Master Agreement.

All initial capitalized terms in this Attachment 3 that are not defined herein shall have the respective meanings given to them in the Participating Addendum, Attachment 1 – State of Michigan Terms and Conditions, or Master Agreement.

END USER LICENSE AGREEMENT

This End User License Agreement (the "Agreement") governs Your Use of Cisco Software and is between You and Cisco. Please read it carefully. The Agreement includes the SEULA(s) located at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html (each, "Supplemental Terms"). Notwithstanding the foregoing sentence, You will not be bound by any terms requiring indemnification by You to third-parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to Your systems; agreeing to be bound by the laws of another state; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the SEULA(s) or any other documents, policies, or terms located in links referenced herein. Capitalized terms are defined in Section entitled "Definitions" and capitalized terms used herein and not defined in "Definitions" will have the meaning given in the Contract; the order of precedence in the event of conflict is in the Participating Addendum. Depending on whether the Software is delivered on-premise as Embedded Software or as a Cisco-hosted cloud offering of Cloud Software, certain terms herein may not apply to Your purchase.

By Using the Software, You agree to the terms of this Agreement. If You determine that You cannot comply with the terms of this Agreement after You have paid for the Software, You may return the Software to the Approved Source, disable, or uninstall the Embedded Software and/or cease Your Use of the cloud-hosted Cloud Software and receive a full refund, provided You do so within thirty (30) days of Your initial purchase.

Section 1. License

a. **License**. Subject to Your payment of the applicable fees to an Approved Source and compliance with this Agreement, Cisco grants You a limited, non-exclusive license to Use the Software and related Documentation for Your internal business purposes only and in accordance with any Supplemental Terms, Order and/or Entitlement. In the event that Cisco requires You to register as an end user, Your license is valid only if the registration is complete and accurate. You and Cisco agree to work in good faith to ensure that any incomplete or inaccurate registrations are resolved to the satisfaction of both parties. The Embedded Software delivered for Use on-premise may contain open source software and is subject to separate license terms. A list of such open-source software and related license agreements can be found at www.cisco.com/go/opensource.

b. **Limitations and Restrictions.** Unless expressly authorized by Cisco in writing, You will not and will not allow a third party you have allowed to Use the Software to:

i. Sell, resell, transfer, sublicense, or assign Your rights under this Agreement to any other person or entity (except as expressly provided in Section 1.f below);

ii. modify, adapt, or create derivative works of the Software or Documentation;

iii. reverse engineer, decompile, decrypt, disassemble or otherwise attempt to derive the source code for the Software, except as authorized by Cisco;

iv. make the functionality of the Software available to third parties in a managed or network provisioned service;

v. Use Software that is licensed for a specific device, whether physical or virtual, on another device;

vi. remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices,or other marks on or within the Software;

vii. Use the Software on secondhand and/or refurbished Cisco equipment; or

viii. Use the Software on third party hardware unless otherwise set forth in the Documentation (or otherwise

authorized by Cisco in writing).

c. Third Party Use of Software. You may allow a third party to Use the Software licensed to You solely (i) on Your behalf, (ii) for Your internal and/or business operations, and (iii) in compliance with this Agreement. You agree that You are responsible for any breach of this Agreement by that third party.

d. Upgrades and Additional Copies. Notwithstanding anything else in this Agreement, You may not Use Upgrades and additional copies of the Software unless You:

i. hold a valid license to the Software, are in compliance with such license, and have paid the applicable fee for the Upgrade; and

ii. purchase the Upgrade separately or have a valid support agreement covering the Software, either as part of a subscription or purchased separately; and

iii. Use additional copies *solely* for backup purposes limited to archiving for restoration purposes.

e. Transferability/Assignment. Except for a transfer or assignment required by law, statute, regulation, legislative action, executive order, or other governmental action, You may only transfer or assign Your license rights to on-premise Embedded Software to another person or entity in accordance with the current Cisco Relicensing/Transfer Policy, and any such transfer or assignment other than in accordance with the Transfer Policy will have no effect. The term "**Affiliate,**" as used in the Transfer Policy and as applied to You, also means any State of Michigan Executive Branch Agency, Department or Division, including the Michigan Department of Attorney General, the Michigan Office of Secretary of State, and the Office of the Governor. Cisco may transfer or assign any of its rights or delegate any of its obligations related to Embedded Software under this Agreement in its sole discretion; however, Cisco must provide written notice to You of such assignment or transfer.

f. Interoperability. If required by applicable law, Cisco will provide You with the interface information needed to achieve interoperability between the on-premise Embedded Software and another independently created program. Cisco will provide this interface information at Your written request after You pay Cisco's licensing fees (if any). You will keep this information in strict confidence according to the terms of this Contract and strictly follow any applicable terms and conditions upon which You and Cisco agree to in writing.

g. Non-production and Trial Use.

i. We may provide beta versions of the Software for you to evaluate and provide feedback. Beta versions are not generally released and may only be used for limited, temporary purposes ("Beta Software"). The Beta Software may not be used in a production environment. Beta Software is unsupported and may contain bugs, errors, and other issues. You accept Beta Software "AS-IS," without warranty of any kind, and Cisco is not responsible for any problems or issues related to Your use. You understand that the Beta Software may never be generally available, and we may discontinue it in our sole discretion at any time for any reason and delete any State Data or other data without liability to You. Your Use of the Beta Software is valid for thirty (30) days from the date it is made available to You. You will be invoiced for the list price if You do not return or stop Using it. You may not publish any results of benchmark tests run on the Beta Software without first obtaining written approval from Cisco.

ii. We may also give You trial access to generally available Software. Any trial period will expire in thirty (30) days unless otherwise stated in writing from Cisco. Trials are also provided "AS-IS" without support or any express or implied warranty or indemnity of any kind. At any time during or at the endof the trial, Cisco may terminate the trial and deactivate or delete Your account and any related data, information, and files, and bar any further access to such data, information, and files for any reason.

Section 2. Ownership and Your Data

a. What We Own. Cisco and its licensors retain ownership of all intellectual property rights in and to the Software and its underlying technology and associated Documentation (together, "Materials"), including all improvements, enhancements, modifications, and derivative works. Cisco reserves all rights to the Materials that are not expressly granted under this Agreement or the Supplemental Terms.

b. What You Own and What You Do with It. You retain all right, title, and interest in and to State Data. You authorize Cisco to use any feedback or ideas You provide in connection with Your Use of the Software for any

lawful purpose. You represent that all account information You provide, to the best of your knowledge, is accurate and will be kept up-to-date and that You will use reasonable means to protect Your account from any unauthorized use or access, and promptly notify Cisco of any such use or access.

c. **How We Use Your Data**. Cisco will process State Data in accordance with Attachment 1 – State of Michigan Terms and Conditions. Cisco will maintain administrative, physical, and technical safeguards consistent with Attachment 1 – State of Michigan Terms and Conditions, which are designed to provide security, confidentiality, and integrity of the State Data we process.

Section 3. Software Support

We will provide basic technical support for subscription Cloud and Embedded Software, as described in the Supplemental Terms. Higher levels of support for subscription Software, and support for perpetual Software is separately available for purchase.

Section 4. Term and Termination

a. Your right to Use the Software begins on the date (i) the on-premise (meaning not installed in a Cisco environment) Embedded Software is made available for download or installation, or (ii) You receive notice that the cloud hosted Cloud Software is provisioned or available for Your use, and continues until the end of the term specified in the Order or Entitlement, unless otherwise terminated in accordance with this Agreement ("Initial Term").

If the Software is licensed for use both on-premise and cloud-hosted, Your right to Use begins on the earlier of the date the Software is made available for download or is ready for provisioning.

b. Software subscriptions will be renewed at the sole election of the State. Your Approved Source will notify You reasonably in advance of any Renewal Term if there are fee changes. The new fees will apply for the upcoming Renewal Term unless You or Your Approved Source promptly notify us in writing, before the applicable renewal date, that You do not intend to renew. In such event, the Software subscription will terminate at the end of the Initial Term.

c. If a party materially breaches this Agreement and does not cure that breach within thirty (30) days after receipt of written notice of the breach, the non-breaching party may terminate this Agreement for cause. Upon termination or expiration of this Agreement, You must cease any further use of the Software and destroy any copies within Your control. Upon any termination by You for Cisco's material breach of the Agreement, You may terminate this Agreement for cause pursuant to Section 23 of the State of Michigan Terms and Conditions, and in addition to any other remedy that may be available to You, we will refund to You either directly or through Your Fulfillment Partner, any prepaid fees covering the remainder of the Term after the effective date of termination. Upon any termination by Cisco for Your material breach of the Agreement, You will pay Cisco or Your Approved Source any unpaid fees covering the remainder of the Term.

d. Cisco reserves the right to end the life ("EOL") of the Software by providing prior written notice by posting at http://www.cisco.com/c/en/us/products/index.html. If You or Your Approved Source prepaid a license fee for Your Use of EOL Cloud Software, Cisco will use commercially reasonable efforts to transition You to a substantially similar Cloud Software. If Cisco does not have a substantially similar Cloud Service, then Cisco will credit You any unused portion of the prepaid fee for such Cloud Service, calculated from the last date the Cloud Service is available. Such credit can be applied towards the future purchase of Cisco products.

Section 5. General Provisions

a. **Audit.** During the license term for the Software and for a period of three (3) years after its expiration or termination, you will take reasonable steps to maintain complete and accurate records of Your use of the Software sufficient to verify compliance with this Agreement. Within thirty (30) days of Cisco's request, but no more than once per year, You shall provide a written certification of Your compliance with the terms of this Agreement for the immediately preceding 12-month period. If You fail to certify, or if Cisco has a good faith belief that Your certification is inaccurate, to the extent permitted by applicable law, and subject to all of Your security procedures and policies, You agree to allow Cisco to audit your compliance with the terms of this Agreement for the immediately preceding 12-month period upon thirty (30) days prior written notice, during normal business hours, and no more than once per year. Any audit shall not unreasonably interfere with your business activities. If the audit discloses underpayment of license fees, You or Your Approved Source will pay undisputed license fees pursuant to the payment provisions of the Contract, and such payment authorized by this section will be the sole and exclusive remedy of Cisco for any underpayment of fees.

b. Survival. Sections 1.b, 2, 4, 5.a, 5.b, 5.d, shall survive termination or expiration of this Agreement.

c. Subcontracting. We may also subcontract any performance associated with the Software to third parties pursuant to Section 10 (Subcontracting) of Attachment 1 - State of Michigan Terms and Conditions. Any such subcontract will not relieve Cisco of any of its obligations under this Agreement.

US Government End Users. The Software and Documentation are "commercial items," as defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software) and Defense Federal Acquisition Regulation Supplement ("DFAR") 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this Agreement may be incorporated, Government end users will acquire the Software and Documentation with only those rights set forth in this Agreement. Any license provisions that are inconsistent with federal procurement regulations are not enforceable against the U.S. Government.

d. Modifications. This Agreement may not be amended except by signed agreement between the parties and attached as a Change Notice.

e. Compliance with Law. You will comply with all applicable laws and regulations related to Your receipt and use of the Software. You must ensure You have the right to use all features of the Software in Your jurisdiction. Cisco will comply with all applicable laws in the provision of the Software to You. We may restrict the availability of the Software in any particular location or modify or discontinue features to comply with applicable laws and regulations. Cisco may also share information as necessary to comply with laws and subject to Section 30.d (Discovery) of Attachment 1 - State of Michigan Terms and Conditions.

f. Integration. If any portion of this Agreement is not enforceable, it will not affect any other terms.

Definitions

"Approved Source" means Cisco or a Cisco authorized reseller, distributor, or systems integrator, including a Fulfillment Partner under this Contract, including the NASPO ValuePoint Master Agreement Terms and Conditions.

"**Authorized User**" means the individuals authorized by You to access the Software.

"Cisco" "we," "our" or "us" means Cisco Systems, Inc. or its applicable affiliate, the Contractor under the NASPO ValuePoint Master Agreement Terms and Conditions.

"Cisco Content" means any Cisco-provided content or data including, but not limited to, geographic and domain information, rules, signatures, threat intelligence or other threat data feeds, suspicious URLs, and IP address data feeds.

"**Cloud Software**" means Cloud Software in the NASPO ValuePoint Master Agreement Terms and Conditions.

"**Confidential Information**" has the meaning in Section 30.a. of Attachment 1 - State of Michigan Terms and Conditions.

"**Documentation**" means the Cisco user or technical manuals, training materials, specifications, privacy data sheets, or other information applicable to the Software.

"**Entitlement**" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification.

"Force Majeure Event" means an event beyond the affected party's reasonable control, including severe weather events, acts of God, actions of any government agency, epidemic, acts of terrorism, or the stability or a portion thereof.

"Cloud Offer Description(s)" means the additional terms and conditions applicable to the specific cloud- hosted Software licensed under this Agreement (located here).

"**Order**" means Software in the NASPO ValuePoint Master Agreement Terms and Conditions.

"SEULA" means the Supplemental End User License Agreement containing additional terms and conditions for the

on-premise Software licensed under this Agreement (located here: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html).

"**Software**" means Software in the NASPO ValuePoint Master Agreement Terms and Conditions.

"**State Data**" has the meaning in Section 29.a. of Attachment 1 - State of Michigan Terms and Conditions.

"**Upgrades**" means all updates, upgrades, bug fixes, error corrections, enhancements, and other modifications to the Software.

"**Use**" or "**Using**" means to download, install, activate, access, or otherwise use the Software

"**You**" or "**Your**" means the Purchasing Entity purchasing the Software pursuant to the NASPO ValuePoint Master Agreement Terms and Conditions and applicable Participating Addendum.

Attachment 4 – Additional Contractor Terms and Conditions

The parties agree that this Attachment 4 – Additional Contractor Terms and Conditions, modifies and replaces Attachment A, Exhibit 2 – Additional Contractor Terms and Conditions (including its attachments), included in the Master Agreement.

All initial capitalized terms in this Attachment 4 that are not defined herein shall have the respective meanings given to them in the Participating Addendum, Attachment 1, or Master Agreement

Services Exhibit

This Services Exhibit governs all Orders for Services placed under this Contract (as defined in the Michigan Participating Addendum). This Services Exhibit consists of the terms set forth in this Attachment 4 (including its attachments) and the Service Description Purchasing Entity may elect to purchase. Notwithstanding the foregoing sentence, Customer will not be bound by any terms requiring indemnification by Customer to third-parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to Customer systems; agreeing to be bound by the laws of another state; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the Service Descriptions or any other documents, policies, or terms located in links referenced herein.

---

1. DEFINITIONS

Terms not defined in the body of the Contract, including the State of Michigan Terms and Conditions and the Master Agreement are those set out in the Glossary of Terms at the end of this Attachment 4.

2. SCOPE

This Exhibit describes the terms and conditions for (a) Direct Purchases from Cisco or Fulfillment Partner by Customer of Services, and (b) delivery by Cisco of the Services according to the options ordered by Customer or otherwise provided by Cisco to Customer. Cisco will provide Services for Products and Customer will be entitled to receive Services for which (i) the applicable Services fees have been paid, (ii) a valid Software license has been granted and (iii) Customer provides information requested by Cisco such as valid serial numbers, site location, contract number, and Product type.

3. PRICING

For direct purchases from Cisco, and subsequent Equipment List renewals, prices for Services shall be those specified in Cisco's then-current Price List less any applicable contract discount in effect under the Contract at the time of acceptance of the Purchase Order by Cisco, or
(b) those set forth in a written price quotation submitted by Cisco or its Fulfilment Partner, if at or below the stated contract discount. All stated prices are exclusive of taxes, fees, and duties or other amounts in accordance with the Contract. Any taxes related to Services purchased pursuant to this Agreement shall be paid by Customer or Customer shall present an exemption certificate acceptable to the taxing authorities. Applicable taxes shall be billed as a separate item on the invoice, to the extent possible. In the event that Customer is unable to provide valid and applicable serial number(s) for Product and Cisco agrees to provide Services, then Service fees payable by Customer shall be at Cisco's then-current time and materials or non-contract service rates. Subject to the price discount floor established by Cisco under the Contract, for indirect purchases, Fulfillment Partners are free to determine their resale prices unilaterally.

Customer understands that no employee or representative of Cisco or anyone else has any authority to determine such resale prices, or to limit the Fulfillment Partners' pricing discretion with respect to Services.

4. INVOICING

Fees for Services, other than those for which a SOW is required, shall be invoiced in advance of

delivery of Services. The timing of invoices for Services provided pursuant to a SOW shall be set forth in the respective SOW.

5. TERM AND TERMINATION

a. The term of Services on an Equipment List shall commence on the date set forth on such Equipment List, which may be up to sixty (60) days following the date of Purchase Order acceptance. The term of Services on an Equipment List shall be for a period of one year, unless otherwise specified on such Equipment List, and may be renewed for additional terms of one or more years at the sole discretion of the State.

b. The term of each SOW shall be stated in the SOW.

c. Cisco reserves the right to make changes to the scope and content of the Services or part thereof, including terminating the availability of a given Service, at any time upon thirty (30) days' prior notice. Such changes will become effective upon renewal of the affected Equipment Lists and SOWs. If Customer does not agree to a change of scope or content, Customer may terminate any affected Equipment List or SOW by notifying Cisco at least sixty (60) days prior to the expiration of the then current one-year term of the Equipment List or SOW. In such case, Cisco shall continue to provide Services until the next expiration date of the affected Equipment List or SOW.

d. Firm Orders for Services under this Services Exhibit placed and accepted prior to expiration of the contract term, (even if involving a multi-year commitment) remain valid in accordance with the contract terms which shall remain binding as to such prior orders only for the term stated therein and shall not otherwise constitute an extension of the Contract and this Services Exhibit for any other Services.

6. [INTENTIONALLY LEFT BLANK]

7. LICENSES

a. Subject to Customer's compliance with the terms of this Services Exhibit, any applicable AS Service Description or SOW, and the End User License Agreement (**EULA**) set forth in Attachment 3 to the Contract, Cisco grants to Customer a worldwide, non-exclusive and non-transferable license to use for Customer's internal business use only: (i) Software provided as a result of Services, if any, solely in object code form; (ii) other Deliverables specified in an applicable AS Service Description or SOW, if any, and (iii) Data Collection Tools, if any (collectively and individually, the "**Licensed Materials**"). In addition, Cisco grants to Customer a right to modify and create derivative works ofany Scripts provided by Cisco to Customer pursuant to this Services Exhibit, solely for Customer'sinternal business use. These license grants do not include the right to sublicense; provided that Customer may permit its suppliers, subcontractors and other related third parties to use the Licensed Materials solely on Customer's behalf for Customer's benefit, provided that Customer ensures that any such use is subject to license restrictions and confidentiality obligations at leastas protective of Cisco's rights in such Licensed Materials as are specified in this Agreement.

b. Nothing in this Agreement, any AS Service Description or any SOW shall alter or affect the Intellectual Property rights and/or licenses provided with any Cisco Products.

c. Customer hereby grants to Cisco a perpetual, irrevocable, royalty free, worldwide right and license to all Intellectual Property in the Customer Feedback (as defined below) to use and incorporate Customer Feedback into any Services, Products, Deliverables, Data Collection Tools, Reports, Scripts or Cisco Pre-Existing Technology, and to use, make, have made, offer to sell, sell, copy, distribute and create derivative works of such Customer Feedback for any and all purposes whatsoever, and Customer acknowledges and agrees that it will obtain no rights in or to any Services, Products, Deliverables, Data Collection Tools, Reports, Scripts or Cisco Pre-Existing Technology as a result of Cisco's use of any such Customer Feedback. For purposes of this Agreement, "**Customer Feedback**" means all oral or written communications regarding improvements or changes to any Services, Products, Deliverables, Data Collection Tools, Reports, Scripts or Cisco Pre-Existing Technology that Customer provides to Cisco.

8. OWNERSHIP

a. Each party will retain the exclusive ownership of all its pre-existing Intellectual Property, Confidential Information and materials, including, without limitation, proprietary ideas, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology that are owned by a party prior to commencement of any Services hereunder, or that are otherwise developed by or for such party outside the scope of this Agreement ("**Pre-Existing Technology**").

b. Except as otherwise expressly set forth in applicable SOW, Cisco owns and will continue to own all right, title and interest in and to the Services, Products, Deliverables, Data Collection Tools, Reports, Scripts, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology provided or developed by Cisco (or a third party acting on Cisco's behalf) pursuant to this Agreement, including modifications, enhancements, improvements or derivative works of any of the foregoing, regardless of who first conceives or reduces to practice, and all Intellectual Property in any of the foregoing (collectively, "**Cisco Intellectual Property**").

c. As between Customer and Cisco, Customer shall at all times retain all right, title, and interest in and to all of Customer's Pre-Existing Technology and all Intellectual Property that is developed by Customer or by a third party on Customer's behalf thereafter, other than Cisco Intellectual Property. Third Party Products shall at all times be owned by the applicable third-party and will be subject to any applicable third-party license terms.

9. SUBCONTRACTING

Cisco reserves the right to subcontract Services to a third-party organization to provide Services to Customer. Any such subcontract shall not relieve Cisco of any of its obligations under this Services Exhibit or the Contract.

GLOSSARY OF TERMS

Additional Services means installation of new Hardware, system additions, Hardware upgrades, dispatch of a field engineer, or non-mandatory engineering changes.

Advance Replacement means shipment of replacement Field-Replaceable Unit (FRU) before receiving failed or defective FRU.

Advanced Services means the Services set forth in the AS Service Description(s) found at http://www.cisco.com/go/servicedescriptions and/or SOW(s) selected by the Customer. Advanced Services does not include Cisco's core maintenance services, such as Smart Net Total Care or Software Application Services, nor does it apply to the purchase, support, or maintenance of any Products.

Advanced Services Engineer means the Cisco engineer appointed to be the main point of contact for a Customer purchasing Advanced Services.

Application Software means non-resident or standalone Software Products listed on the Price List that include but are not limited to Cisco Systems® Network management Software, security Software, IP telephony Software, Internet appliance Software, Cisco® Intelligent Contact Management Software, IP Contact Center Software, and Cisco Customer Interaction Suite Software.

AS Service Descriptions mean the description of the Advanced Services available from Cisco, which are available at http://www.cisco.com/go/servicedescriptions and which are incorporated in this Agreement by reference.

Authorized Channel means a system integrator, distributor or reseller authorized by Cisco to sell Services.

Business Days means the generally accepted days of operation per week within the relevant region where the Services shall be performed, excluding local holidays as observed by Cisco.

Cisco means Contractor under the NASPO Master Agreement.

Customer means Purchasing Entity under the NASPO Master Agreement.

Data Collection Tools means Hardware and/or Software tools that support Cisco's ability to provide troubleshooting on cases, data analysis, and report generation capabilities as part of the Advanced Services.

Depot Time or **Local Time** means Central European Time for Services provided in Europe-Middle East and Africa, Australia's Eastern Standard Time for Services provided in Australia, Japan's Standard Time for Services provided in Japan, and Pacific Standard Time for Services provided in all other locations.

Deliverable(s) means, with respect to each AS Service Description and/or SOW, the items to be delivered by Cisco to Customer as set forth in an applicable AS Service Description and/or SOW, including, without limitation, any Software, Reports, Data Collection Tools, and/or Scripts.

Device Type means a Cisco supported Hardware Product (for example, Cisco Catalyst® 6509 Switch, GSR 12000 and Cisco 7200 Series Router).

Direct Purchases means purchases of Services by Customer directly from Cisco.

Equipment List means the list of Hardware and/or Software on a Purchase Order for which Cisco provides services.

Event means notification by Customer of its performance of a planned Network Hardware, Software, or configuration change.

Feature Set Upgrade means a separately licensed and priced Software release that contains an enhanced configuration or feature set.

Field-Replaceable Unit (FRU) means any component or subassembly of an item or unit of Hardware that reasonably can be replaced at Customer's location. FRUs also may be subject to size and weight limitations.

Four-hour Response means:

(i) For Advance Replacement Service, the four-hour time period commences upon the Cisco problem diagnosis and determination that a FRU is required and ends when the FRU is delivered onsite.

(ii) For onsite service, the four-hour time period commences upon the Cisco problem diagnosis and determination that remedial onsite service is required and ends when Cisco personnel arrive onsite.

Indirect Purchases means purchases of Services by Customer through an Authorized Channel.

Intellectual Property means any and all tangible and intangible: (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms, and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter inforce (including any rights in any of the foregoing).

Level 1 means support that is defined as having the necessary technical staff (Cisco or Cisco-authorized reseller) with appropriate skill, perform installations, Remedial Hardware Maintenance, and basic Hardware and Software configuration on Cisco Products.

Level 2 means support that is defined as having the necessary technical staff with the appropriate skills to perform isolation, replication, and diagnosis of internet-based problems on Cisco Product(s). Customershall not report Software bugs to Cisco prior to attempting to identify the source of such bugs and testing in Customer's Network where appropriate. If the Customer cannot duplicate the bug in Customer's Network, Customer and Cisco shall cooperate in attempting to replicate and resolve related Software bugs in either Customer's or Cisco's test facility as mutually agreed. In all cases Customer will address Software bugs on a best effort basis to replicate same in Customer's Network and document activity to Cisco before seeking further resolution with Cisco's participation.

Local Time means local time on Business Days.

Maintenance Release means an incremental Software release that provides maintenance fixes and may

provide additional Software functions. Cisco designates Maintenance Releases as a change in the digits to the right of the tenths digit or of the hundredths digit of the Software version number [x.x.(x) or x.x.x.(x)].

Major Release means a release of Software that provides additional software functions. Cisco designates Major Releases as a change in the ones digit of the Software version number [(x).x.x].

Minor Release means an incremental release of Software that provides maintenance fixes and additional Software functions. Cisco designates Minor releases as a change in the tenths digit of the Software version number [x.(x).x].

Network means a set of interconnected and interworking Cisco supported Hardware and Software that is implemented, operated, and supported by Customer from a single network operations center (NOC).

Network Infrastructure means your core transport and aggregation Network technology (for example, metro optical, ATM/Frame Relay, IP core and Cisco security devices including, but not limited to, Firewall, IDS and VPN3000).

Network Infrastructure Size means the total value of Products in Customer's Network based on the global list price of the Products that Customer has purchased.

Remedial Hardware Maintenance means diagnosis and onsite replacement of Hardware components with FRUs.
Reports means reports, recommendations, network configuration diagrams, and related non-Software Deliverables provided by Cisco to Customer pursuant to this Agreement.

Scripts means software scripts, macros and batch files provided by Cisco to Customer pursuant to this Agreement.

Services means one or more of the services options selected by the Customer in its Purchase Order and described at: http://www.cisco.com/go/servicedescriptions

Services Descriptions mean the detailed descriptions of the Services purchased by Customer which are incorporated into this Services Exhibit by reference.

Standard Business Hours means (i) 8:00 AM to 5:00 PM, Depot time, on Business Days for replacement of failed Products and (ii) 8:00 AM to 5:00 PM, Local Time at location of the respective Cisco TAC, on Business Days for case handling of TAC calls.

TAC means the Cisco Technical Assistance Center.

Technical Support Services means Services that provide both essential proactive and reactive operation and maintenance support Services identified as Technical Support Services at http://www.cisco.com/go/servicedescriptions.

Technology Application means specific technologies including, but not limited to, content networking, broadband, and IP telephony that do not operate at the Network Infrastructure level.

Third Party Products means third party hardware and/or software, and all upgrades/updates thereto, that are designated by Cisco as required for:

(i) The operation of Application Software in conformance with Cisco applicable Application Software Documentation; and

(ii) Cisco support of the Application Software.

Transactional Advanced Services means the project related or consultancy Services sold under a Statement of Work.

Two-hour Response means:

(i) For Advance Replacement, the two-hour time period commencing with Cisco’s problem diagnosis and determination that a FRU is required and ending when the FRU is delivered onsite.

(ii) For onsite service, the two-hour time period commencing with our problem diagnosis and determination that remedial onsite service is required and ending when Cisco personnel arrive onsite.

Update means Cisco Software Maintenance Releases, Minor Releases and Major Releases containing the same configuration or feature set as originally acquired, unless the Customer has upgraded the applicable Hardware or Software to a configuration or feature set other than what was originally acquired, and the applicable license fee for that upgrade has been paid. Updates do not include Feature Set Upgrades.

CISCO SEVERITY AND ESCALATION GUIDELINES

Customer shall assign a severity to all problems submitted to Cisco.

Severity 1 means an existing Network is down or there is a critical impact to Customer's business operation. Customer and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means operation of an existing Network is severely degraded or significant aspects of Customer's business operation are negatively impacted by unacceptable Network performance. Customer and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means operational performance of the Network is impaired, although most business operations remain functional. Customer and Cisco both are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.

Severity 4 means information is required on Application Software capabilities, installation, or configuration. There is little or no impact to Customer's business operation. Customer and Cisco both are willing to provide resources during Standard Business Hours to provide information or assistance as requested.

If you do not believe that adequate progress is being made or that the quality of Cisco service is satisfactory, we encourage you to escalate the problem to the appropriate level of management by asking for the TAC duty manager.

Cisco Escalation Guideline

*Elapsed Time**	*Severity 1*	*Severity 2*	*Severity 3*	*Severity 4*
1 hour	Customer Engineering Manager			
4 hours	Technical Support Director	Customer Engineering Manager		
24 hours	Vice President, Customer Advocacy	Technical Support Director		
48 hours	President/CEO	Vice President, Customer Advocacy		
72 hours			Customer Engineering Manager	
96 hours		President/CEO	Technical Support Director	Customer Engineering Manager

*Severity 1 escalation times are measured in calendar hours—24 hours per day, 7 days per week. Severity 2, 3, and 4 escalation times correspond with Standard Business Hours.

SERVICES NOT COVERED

Services that are not expressly set forth in the applicable Service Description or Statement of Work document are not covered under such Service Description or Statement of Work, including, without limitation, the following:

1. Services are only provided for generally available Products and Software releases/versions, unless agreed otherwise.
2. Any customization of, or labor to install, Software and Hardware (including installation of Updates).
3. Furnishing of supplies, accessories, or the replacement of expendable parts (e.g., cables, blowerassemblies, power cords, and rack mounting kits).
4. Electrical or site work external to the Products.
5. Service for Hardware that is installed outdoors or that is installed indoors but requires special equipment to perform such Service.
6. Hardware replacement in quantities greater than three (3) FRUs, including those replacements due to pervasive issues documented in an engineering change notice or field alert unless End User has troubleshot failed Hardware down to the FRU level.
7. Services performed at domestic residences.
8. Support or replacement of Product that is altered, modified, mishandled, destroyed or damaged by one or more of the following: (a) natural causes; (b) environmental failures; (c) your failure to take any required actions; (d) a negligent or willful act or omission by you or use by you other than as specified in the applicable Cisco-supplied documentation; or (e) an act or omission of a third party (except for Cisco Fulfillment Partners, subcontractors or other third parties contracted by Cisco).
9. Services or software to resolve Software or Hardware problems resulting from third party product or causes beyond Cisco's control or failure to perform your responsibilities set out in this document.
10. Services for non-Cisco Software installed on any Cisco Product.
11. Any Hardware or third-party product upgrade required to run new or updated Software.
12. Erasure or other removal of any customer or third-party data on Products (or parts thereof) returned, repaired, or otherwise handled by Cisco.
13. Additional Services are provided at the then-current time and materials rates.
14. Except as otherwise agreed, Software entitlement, including media, documentation, binary code, source code or access in electronic or other form is not provided. In addition, except as otherwise provided, no right, use or license to our Software is granted and you acknowledge and agree that you obtain no such rights.
15. Application Software is not supported as part of the SMARTnet support services provided by Cisco and is only supported under a separate service description.

The non-entitlement policies posted at http://www.cisco.com/go/warranty are hereby incorporated into this Agreement by this reference.

Capitalized terms are defined in the Glossary of Terms or may be as set forth in the applicable Service Description or Statement of Work.

Attachment 5 – State of Michigan Service Level Agreement

CONTRACT PERFORMANCE - METRICS

The State and the Contractor will monitor performance throughout the course of this Contract.

The Contractor will monitor the performance and coverage of all warranty and maintenance services. In addition to monitoring of repair cases, the Contractor will meet regularly with Fulfillment Partners to discuss performance metrics, issues affecting the industry or clients, new initiatives, and new innovations in technology. The primary focus is on making sure service commitments are met or exceeded.

Contractor will provide the Services according to the metrics detailed in the Service Level Table below. Metrics will be completed with the following operational considerations:

Service Level Table		
I: Service Metric #	**II: Service**	**III: State Minimum Metric**
A1	Accuracy of CISCO Hardware and Software	The State expects 100% accuracy of CISCO Hardware and Software delivered as defined in the bill of materials provided by CISCO or its Fulfillment Partners.
A2	Warranty & Maintenance: critical (hardware)	4-hour response, 24x7 when the State has purchased '4-hour response, 24x7' response time for a specific offer available under the Contract
A3	Warranty & Maintenance: Standard (hardware)	Next Business Day response when the State has purchased 'Next Business Day' response time for a specific offer available under the Contract.
A4	ITAM documentation accuracy	The State expects 100% accuracy of ITAM documentation.

SERVICE LEVEL CREDITS

Contractor will report quarterly following the execution of the Participating Addendum, on all Service Metrics defined above ("Service Level Report"). Such report must be in electronic or such other form as the State may approve in writing and shall include for each Service Metric, at a minimum: (a) the actual performance for each Service Metric relative to the Minimum Metric Requirement; (b) the Service Level Credit due to the State for each Service Metric (if any); and (c) if Service Level Credits are due to the State, a description of the cause of the performance issues and any corrective actions to resolve the issues.

Service Level Credits. Failure to achieve any of the State Minimum Metric requirements identified in the table above will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in the Service Level Credits Table below in accordance with payment terms set forth in the Contract

Service Level Credits Table			
I: Service Metric#	**II: Service**	**III: Quarterly SLA/SLT (% of purchase orders)**	**IV: Service Level Credit**
A1	Accuracy of CISCO Hardware and Software	Less than or equal to 95%	10% of all inaccurate line items.
A2	Warranty & Maintenance: critical(hardware)	Less than or equal to 90%	$500 per late response based on service level target
A3	Warranty & Maintenance: Standard(hardware)	Less than or equal to 90%	$500 per late response based on service level target
A4	ITAM documentation accuracy	Less than or equal to 95%	10% of all inaccurate line items.

Compensatory Purpose. The parties intend that the Service Level Credits constitute compensation to the State, and not a penalty. The parties acknowledge and agree that the State's harm caused by Contractor's delayed delivery of the Services would be impossible or very difficult to accurately estimate as of the Effective Date, and that the Service Level Credits are a reasonable estimate of the anticipated or actual harm that might arise from Contractor's breach of its Service Level obligations.

Issuance of Service Credits. Contractor shall, for each quarterly reporting period, issue to the State, together with Contractor's Service Level Report for such period, a written acknowledgment setting

forth all Service Level Credits to which the State has become entitled during that invoice period. Contractor shall pay the amount of the Service Level Credit as a debt to the State within fifteen (15) Business Days of issue of the Service Level Credit acknowledgment, provided that, at the State's option, the State may, at any time prior to Contractor's payment of such debt, deduct the Service Level Credit from the amount payable by the State to Contractor pursuant to such invoice.

Additional Remedies for Service Level Failures. Contractor's repeated failure to meet the Service Levels set out in the Service Level Table will constitute a material breach under the Contract. Without limiting the State's right to receive Service Level Credits under this Section, the State may terminate this Contract for cause in accordance with terms of the Contract.

Attachment 6 - Personal Data Brief

Cisco is committed to protecting and respecting Personal Data, no matter where it comes from or where it flows. When we refer to Personal Data (also referred to as Personally Identifiable Information) we mean any information relating to an identified or identifiable natural person (for more information click here).

Our Global Personal Data Protection and Privacy Policy demonstrates our commitment to protecting Personal Data and complying with applicable laws regarding Personal Data. In that Policy, we commit to the following principles regarding Personal Data:

- **Fairness.** We will process Personal Data in a lawful, legitimate, and transparent manner.
- **Purpose Limitation.** We will only collect Personal Data for specific, explicit, and legitimate purposes. Any subsequent processing should be compatible with those purposes, unless we have obtained the individual's consent, or the processing is otherwise permitted by law.
- **Proportionality.** We will only process Personal Data that is adequate, relevant, and not excessive for the purposes for which it is processed.
- **Data Integrity.** We will keep Personal Data accurate, complete, and up to date as is reasonably necessary for the purposes for which it is processed.
- **Data Retention.** We will keep Personal Data in a form that is personally identifiable for no longer than necessary to accomplish the purposes, or other permitted purpose(s), for which the Personal Data was obtained.
- **Data Security.** We will implement appropriate and reasonable technical and organizational measures to safeguard Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use, or access. We will instruct and contractually require third parties processing Personal Data on behalf of Cisco, if any, to: (a) process it only for purposes consistent with Cisco's purposes for processing; and (b) implement appropriate technical and organizational measures to safeguard the Personal Data.
- **Individual Rights.** We will process Personal Data in a manner that respects individuals' rights under applicable data protection laws.
- **Accountability.** We will implement appropriate governance, policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of Personal Data is in accordance with our Global Personal Data Protection and Privacy Policy and applicable data protection laws.

Why we process Personal Data

The following key objectives form the basis of how and when we use Personal Data:

Objective	Summary
Solution Delivery	Personal Data may be used to operate our products and deliver services to you with critical and timely system insights. For example, our Cloud offers depend on proper user authentication. Personal Data is also needed for us and our partners to provide you with warranty support, technical support, and other services.
Accelerate Adoption	Our products and services contain various features that you can employ to best address your business objectives. We work closely with your organization to accelerate your time to realize the value of our products and services, provide consultation, recommendations, expert insights, analysis, and training so you can best utilize the many features of our products and services in a way that best meets your needs.
Trusted Relationship	We view ourselves as a trusted advisor to you and maintain a number of relationships within your organization. We need these contacts for a number of purposes, such as to advise and guide you in your buying decisions, to keep you up to date on renewals, and to ultimately help you transact business with us and your partners or distributors (if any).
Solution Improvements	Our solutions must evolve and improve to meet our customers' changing needs. These improvements are guided by the insights gained from Systems Information that show us how our solutions are working and being used. If Personal Data is received in connection with Systems Information, we will treat that data as you would expect - as Personal Data, not as Systems Information - and always consistent with applicable law and your contracts or agreements with us.

Our Privacy Data Sheets and Privacy Data Maps

We maintain Privacy Data Sheets and Privacy Data Maps on the Cisco Trust Portal for specific products and services that provide you with additional information such as what Personal Data we process, where and for how long we store the information, and what sub-processors we may use.

Our Master Data Protection Agreement

When Cisco is acting as data processor (i.e., managing Personal Data on behalf of our customers), our Master Data Protection Agreement (MDPA), applicable Privacy Data Sheets and our Online Privacy Statement provide details about our commitments regarding our processing of Personal Data when you use our products and services. Our MDPA is publicly available on the Cisco Trust Center (here). Key elements in the MDPA include:

- terms and conditions consistent with the principles in this document that will govern the processing of Personal Data;
- technical and organizational security measures that will be implemented to minimize the risk of accidental loss, destruction, alteration, unauthorized disclosure, unauthorized access, or unlawful destruction of Personal Data; and
- incorporation of the European Union Standard Contractual Clauses, and APEC Cross Border Privacy Rules system requirements for international data transfers.

Our Online Privacy Statement

When you access our websites or use one of our solutions, our Online Privacy Statement describes how we handle Personal Data and provides the choices available to you regarding our collection, use, and access to that information.

Sharing Personal Data

We require our suppliers and contractors to adhere to applicable data protection laws and terms and conditions consistent with the principles in this document when handling Personal Data on our behalf by signing our Supplier MDPA, which is publicly available here.

Similarly, we require all of our partners and distributors to comply with applicable laws, including privacy and data protection laws, and the confidentiality provisions in our agreement with them.

How Individuals can control their Personal Data

We respect the rights of individuals regarding their Personal Data. We provide a Cisco Profile Management Tool that allows you to view, edit and set the preferences related to the Personal Data in for your Cisco profile. We also provide a Privacy Request Form to assist you and your end users with any inquiries about your Personal Data and process requests, such as to opt-out from communications etc.

Our Information Security Program

We maintain a robust Information Security Program. For detailed information, please click here.

Data Transfer Mechanisms

We have invested in the following transfer mechanisms when transferring Personal Data across jurisdictions:

- EU Standard Contractual Clauses
- Binding Corporate Rules for Controllers
- Binding Corporate Rules for Processors (pending approval)
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors

Breach Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. Our Incident Commander directs and coordinates our response, using diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG). For additional information regarding our breach notification process, please see Cisco's MDPA here.