STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **MA240000000551**

CONTRACTOR	
	Escape Velocity Holdings, Inc
	5555 Corporate Exchange Court SE
	Grand Rapids MI 49512
	Tammie Buehler
	616-901-9509
	Tammie.Buehler@Trace3.com
	VS0101291

STATE			
	Program Manager	Stephanie Jeppesen	DTMB
		517-335-6899	
		JeppesenS@michigan.gov	
	Contract Administrator	Kristine Mills	DTMB
		517-242-6402	
		millsk11@michigan.gov	

CONTRACT SUMMARY			
Intrusion Prevention System			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
April 9, 2024	April 8, 2027	7 - 12 Months	April 8, 2027
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS		**EXTENDED PURCHASING**	
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other		☒ Yes ☐ No	
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$1,642,431.91	$0.00	$1,642,431.91

DESCRIPTION
Effective 6/16/2025, the parties add the following language to the Contract: "Accessibility Requirements. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites, applications, content, and electronic documents. Due to a change in the law, the State is required to comply with specific accessibility standards for websites, applications, content and documents. Starting 4/24/2026, throughout the Term, all websites, applications, software, content, and electronic documents, including but not limited to mobile applications, text, images, sounds, videos, controls, animations, links, and documents (including files in the following formats: PDF, word processing, presentation, and spreadsheet), created, provided, or made available by the Contractor under this Contract, must comply with WCAG 2.1 Level AA." All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency and DTMB procurement.

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **MA240000000551**

CONTRACTOR	
	Escape Velocity Holdings, Inc
	5555 Corporate Exchange Court SE
	Grand Rapids MI 49512
	Tammie Buehler
	616-901-9509
	Tammie.Buehler@Trace3.com
	VS0101291

STATE			
	Program Manager	Stephanie Jeppesen	DTMB
		517-335-6899	
		JeppesenS@michigan.gov	
	Contract Administrator	Kristine Mills	DTMB
		517-242-6402	
		millsk11@michigan.gov	

CONTRACT SUMMARY

Intrusion Prevention System

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
April 9, 2024	April 8, 2027	7 - 12 Months	April 8, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other	☒ Yes ☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$1,640,490.95	$1,940.96	$1,642,431.91

DESCRIPTION

Effective 3/28/2025, the parties agree to add $1,940.96 for the services detailed in the Firepower Co-term quote attached. All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

TRACE3

State of Michigan Firepower Co-term

Quote # Trace3.145262.v1

Prepared for:

State Of Michigan

Katie LaHaye
LaHayeK@michigan.gov

5555 Corporate Exchange Court SE
Grand Rapids, MI 49512

Modify Sub1499043

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
1	1	FTDV-SEC-SUB	Cisco Firepower TD Virtual Subscription	4/9/2025	4/8/2027	$0.00	$0.00
2	1	SVS-FTDV-SEC-M	Embedded Online Support for Cisco Firepower TD Virtual	4/9/2025	4/8/2027	$0.00	$0.00
3	2	FTD-V-5S-TMC	Cisco Firepower TD Virtual TP, Malware & URL Lic, 100 Mbps	4/9/2025	4/8/2027	$377.00	$754.00
4	2	FTD-V-5S-BSE-K9	Cisco Firepower TD Virtual Base Lic, 100 Mbps	4/9/2025	4/8/2027	$652.00	$1,304.00
5	1	DISCOUNT - CISCO	Credit for existing coverage 4/9/2025-7/22/2025			($283.03)	($283.03)
24 Months, Prepaid							

Subtotal: **$1,774.97**

Smartnet Co-term

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
1	1	CON-ECMUS-SFMMCVWK	Cisco Firepower Management Center, (VMWare) for 2 devices Location: DIMONDALE	8/29/2025	4/8/2027	$165.99	$165.99

Subtotal: **$165.99**

5555 Corporate Exchange Court SE
Grand Rapids, MI 49512

State of Michigan Firepower Co-term

Prepared by:

Trace3 - Grand Rapids

Tammie Buehler
tammie.buehler@trace3.com

Prepared for:

State Of Michigan

608 W Allegan St
1st Floor
Lansing, MI 48933
Katie LaHaye
(517) 335-5756
LaHayeK@michigan.gov

Quote Information:

Trace3.145262.v1

Quote Date: 03/13/2025
Expiration Date: 04/10/2025

Quote Summary

Description	Amount
Modify Sub1499043	$1,774.97
Smartnet Co-term	$165.99
Total:	**$1,940.96**

Upon client signatory's execution of this Quote, he/she affirms that:

1. Client will purchase and pay Trace3 for the equipment and/or services referenced above;
2. He/she is authorized to accept this Quote on behalf of client and has complied with all of client's business practices in making this purchase;
3. Quoted amounts exclude sales taxes, which will be charged on all U.S. shipments; and
4. Client is responsible for submitting exemption certificates for sales tax-exempt purchases.
5. Use of the equipment and/or services referenced above is subject to the applicable end-user license agreement of the manufacturer.

State Of Michigan

Signature: _____

Name: _____

Title: _____

Date: _____

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **MA240000000551**

CONTRACTOR	
	Trace3, LLC
	5555 Corporate Exchange Court SE
	Grand Rapids MI 49512
	Tammie Buehler
	616-901-9509
	Tammie.Buehler@Trace3.com
	VS0101291

STATE			
	Program Manager	Stephanie Jeppesen	DTMB
		517-335-6899	
		JeppesenS@michigan.gov	
	Contract Administrator	Jarrod Barron	DTMB
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY

Intrusion Prevention System

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
April 9, 2024	April 8, 2027	7 - 12 Months	April 8, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other	☐ Yes ☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$1,403,193.44	$237,297.51	$1,640,490.95

DESCRIPTION

Effective 06/21/2024, the parties add $237,297.51, $213,218.00 for the services detailed in the attached statement of work and $24,079.51 for the ongoing maintenance and support services listed in the attached Cisco Extended FirePower Support quote. All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, and DTMB Central Procurement approval on 6/21/2024. Remaining Ad Board funds after this contract change notice: $12,702.48.

MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK

Project Title: **FirePower Replacement Implementation, & Staff Augmentation**	**Period of Coverage:** **06/17/24 – 02/28/25**
Requesting Department: **Cybersecurity and Infrastructure Protection**	**Date:** **06/11/2024**
Agency Project Manager: **TBD**	**TBD**
DIT Contract Liaison: **Stephanie Jeppesen**	**TBD**

BACKGROUND:
This Statement of Work (SOW) is subject to the terms and conditions of Contract 171-220000001151.

The State has already purchased eight (8) Cisco FPR3140 Intrusion Prevention System ("IPS") and one (1) Cisco FMC4700 management appliance from Trace3 to replace the existing eight (8) FirePower 8350 IPS and one (1) FMC4500 management console in the two (2) Michigan datacenters and these need to be implemented and migrated away in production today. In addition, the SOS primary Firewall ("FW") IPS administrator will be leaving that role on June 24th. The State requires the migration project to start prior to June 24th. Trace3 will supply a Security Engineer to assist with conducting knowledge transfer with that existing IPS administrator and provide remote support as the State completes the implementation and integration of the new hardware. Trace3 will provide 30 days of support as well to address questions on the implementation and migration that the State may have. In addition, Trace3 will also be providing a 6-month staff augmentation role for the NGIPS administrator role gap to manage the new Cisco FPR3140 IPS sensors and FMC4700 management appliance as well as provide general cybersecurity knowledge and tools as the State requires.

PROJECT OBJECTIVE:
- Trace3 Security Engineer will provide migration support for Production NGIPS From (8) Cisco 8350 and (1) Cisco FMC4500 to (8) Cisco FPR3140 and (1) Cisco FMC4700.
- Trace3 Security Engineer will provide 30-Days of Support After Migration.
- Transition New Cisco NGIPS Environment to Trace3 Staff Augmentation Role

IN-SCOPE SITES:
- Lansing Datacenter ("DC")
- Grand Rapids DC

IN-SCOPE HARDWARE:
- Eight (8) new Cisco FPR3140 IPS
- One (1) new Cisco FMC4700
- Eight (8) existing Cisco FirePower 8350 IPS
- One (1) existing Cisco FM4500 management console
    - Includes existing 3rd party rules that will be migrated over

SCOPE OF WORK:

A. Structured support based project (the "Project"):
   - Initiate/Ongoing Governance
     - Internal Call
     - External Call
     - Weekly Status Call/Meetings (eight) 8 Week project)
   - Execute
     - Provide configuration support of one (1) FMC4700 Management Plane including latest stable software image, Cisco Smart License Assignment, Threat Prevention Services, etc.
     - Provide configuration support of eight (8) FPR3140 Management Plane including Latest Stable Software Image, Cisco Smart License Assignment, Threat Prevention Services, etc.
     - Support the State as they replace existing eight (8) 8350 IPS with eight (8) FPR3140 IPS that are currently in-line with the State's firewall; approximately the weekend of June 22-23.
     - Provide day-2 support of the active IPS mode of the eight (8) FPR3140 IPS appliances ensuring adequate behavior and action taking by June 24, 2024.
     - Provide up to thirty (30) days of support until staff augmentation role is integrated into Client team.
   - Closure
     - Trace3 Security Engineer to Trace3 six (6) month Staff Augmentation Transition
     - Project Closure Meeting

B. Staff Augmentation for six (6) months
   - Scope
     - Network Design and Implementation: Design and implement scalable, secure, and efficient network architectures that meet business requirements.
     - Cisco Firepower Expertise: Utilize extensive knowledge of Cisco Firepower to configure and manage firewall policies, intrusion prevention systems, and advanced threat protection.
     - Security Management: Develop and enforce security policies, procedures, and protocols to protect network infrastructure from internal and external threats.
     - Performance Optimization: Monitor and optimize network performance, ensuring minimal downtime and maximum efficiency.
     - Technical Leadership: Provide technical leadership and mentorship to junior network engineers, fostering a culture of continuous learning and improvement.
     - Incident Response: Lead incident response efforts for network security breaches, performing root cause analysis and implementing corrective measures.
     - Collaboration: Work closely with cross-functional teams, including IT, security, and operations, to align network architecture with business goals.
     - Documentation: Maintain comprehensive documentation of network designs, configurations, and processes.

ASSUMPTIONS:

- Trace3 will be engaged for an eight (8) week migration Project timeline.
- The State will clearly define Project timelines to ensure Trace3 scopes the level of effort into this Project.
- Trace3 Security Engineer will be "shoulder surfing" meaning provide support and escalation support over a screen-share, so not required to be onsite at Client datacenters or require direct VPN access into the Client environment.
- The State may request on-site support for emergencies, but it is not expected.
- Staff Augmentation Assumptions

- The State will directly manage the task list being provided to the Trace3 engineer and the concomitant outcomes and Deliverables.
- The State will provide the resources with any necessary equipment required to perform the hours of service in a timely manner.
- Trace3 Security Engineer is expected to have, but not guaranteeing all of, the following:
  - Certifications: Relevant certifications such as Cisco Certified Network Professional ("CCNP") Security, Cisco Certified Internetwork Expert ("CCIE") Security, and/or Cisco Firepower Threat Defense ("FTD").
  - Technical Skills:
    - Extensive knowledge of Cisco Firepower Management Center ("FMC") and Firepower Threat Defense (FTD).
    - Proficiency in designing and implementing network security solutions, including firewalls, Virtual Private Networks ("VPNs"), and intrusion detection/prevention systems.
      - Strong understanding of network protocols, routing, and switching.
      - Experience with network monitoring and management tools.

- Any other provision of this SOW notwithstanding, either the Client or Trace3 shall have the right, within its sole discretion, to terminate the Services without further liability hereunder for any reason whatsoever upon thirty (30) days prior written notice to the Client or Trace3. In such event, Client shall only be liable to Trace3 for Fees earned and expenses incurred for the Services properly performed prior to such notice.

DELIVERABLES:

Project:

Trace3 Security engineer provides best-effort support and escalation support as defined above given the short timeframe to migration prior to June 24, 2024.

Staff Augmentation:

This SOW provides a not to exceed number of hours, as listed below for the supplied Trace3 resource to provide services to the Client in the areas identified under the Staff Augmentation Scope. Trace3's Deliverable is the completion of hours or when the State accepts the Deliverables, whichever comes first. Specific deliverables will be defined as needed by the State throughout the term of the engagement.

ACCEPTANCE:

Hours of service delivered by Trace3 will be subject to Acceptance by the State as specified in Contract 171-220000001151.

OUT OF SCOPE:

- Knowledge transfer or documentation will not be provided as part of this time and materials project.
- Configuration of the existing eight (8) Cisco 8350 IPS appliances and one (1) Cisco FMC4500 management appliance for the exception of migration configurations to new eight (8) Cisco FPR3140 and one (1) Cisco FMC4700 management appliance.
- Configuration or troubleshooting outside of the defined Cisco NGIPS appliances within this scope.

PROJECT CONTROL AND REPORTS:

In accordance with the Contract, Trace3 will provide weekly project status reports to the State from Project kickoff until final acceptance.

PAYMENT SCHEDULE:

Payment will be made on a not to exceed time and materials basis. Contractor may invoice the State up to $213,218 on a bi-weekly basis after the State formally accepts the deliverables, adhering to the invoicing provisions in the Contract terms and conditions.

Services	Rate	Not to Exceed Quantity	Fee Component
Professional Services			
Security Engineer	$186 / hour	148 hours	$27,528
Staff Augmentation Security Engineer Resource	$186 / hour	960 hours	$178,560
Project Management	$155 / hour	46 hours	$7,130
		Total Not to Exceed Estimated Fee:	**$213,218**

EXPENSES:
The State will NOT pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:
The designated Agency Project Manager is:
TBD

The designated DTMB Project Manager is:
Stephanie Jeppesen
Michigan Department of Technology, Management and Budget
530 West Allegan Street
Lansing, MI 48909
jeppesenS@michigan.gov

The designated Trace3 Project Manager is (during the Project part of the scope only):
Marisa Miller, CSM
Marisa.miller@trace3.com
470-701-2207

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:
Contractor will perform work remotely.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:
Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing. No overtime will be permitted.

Cisco Extended FirePower Support Quote
2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
1	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510301 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
2	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510298 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
3	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510317 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
4	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510341 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92

2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
5	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510339 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
6	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000113510319 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
7	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114020454 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
8	1	CON-LSW-1	^^^Cisco FirePOWER 8350 Chassis, 2U, 7 Slots Serial #: 13111500200003-P **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$2,300.65	$2,300.65
9	1	CON-LSW-1	^^^Cisco FirePOWER 8350 Chassis, 2U, 7 Slots Serial #: 13111500200088-P **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$2,300.65	$2,300.65

2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
10	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114170587 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
11	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114141203 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
12	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114170546 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
13	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114230535 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92

2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
14	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114230617 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
15	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114230561 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
16	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: SMAAMDA0031-000114230496 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
17	1	CON-LSW-1	^^^Cisco FirePOWER 40G Stacking Kit for 8300 Serial #: 14043000400027-C **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$5,477.86	$5,477.86
18	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92

2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
19	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
20	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
21	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
22	1	CON-LSW-1	^^^Cisco FirePOWER 8350 Chassis, 2U, 7 Slots Serial #: 14032100200085-P **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$2,300.65	$2,300.65
23	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92

2 Months

Line #	Qty	Part Number	Product Details	Start Date	End Date	Unit Price	Extended Price
24	1	CON-LSW-1	^FirePOWER 2-Port 10 Gbps SR Fiber Network Module with Bypass Serial #: $0.00 **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$354.92	$354.92
25	1	CON-LSW-1	^^^Cisco FirePOWER 8350 Chassis, 2U, 7 Slots Serial #: JMX1913804A **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$2,300.65	$2,300.65
26	1	CON-LSW-1	^^^Cisco FirePOWER 8350 Chassis, 2U, 7 Slots Serial #: 14032100200095-P **End of Support: 06/30/2024** Location: LANSING	7/1/2024	8/31/2024	$2,300.65	$2,300.65

Subtotal: **$24,079.51**

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management & Budget
320 S. Walnut Street, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171-240000000551**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	
	Trace3, LLC
	5555 Corporate Exchange Court SE
	Grand Rapids, MI 49512
	Tammie Buehler
	616-901-9509
	Tammie.Buehler@Trace3.com
	CV0013492

STATE			
	Program Manager	Stephanie Jeppesen	DTMB
		517-335-6899	
		jeppesens@michigan.gov	
	Contract Administrator	Jarrod Barron	DTMB
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Intrusion Prevention System			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
4/9/2024	4/8/2027	Seven 1-Year (Through 4/8/2034)	N/A
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Payment Request (PRC) ☐ Other			☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
New contract established via RFS 171-230000002943. Approved by State Administrative Board on 4/9/2024.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$1,403,193.44**

SOFTWARE CONTRACT TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this "Contract") are agreed to between the State of Michigan (the "**State**") and Trace3, LLC ("**Contractor**"), a California limited liability company. This Contract is effective on April 9, 2024 ("**Effective Date**"), and unless terminated, will expire on April 8, 2027 (the "**Term**").

This Contract may be renewed for up to 7 additional 1-year period(s) (potentially through 4/8/2034). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via a Change Notice.]

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

"**Acceptance**" has the meaning set forth in **Section 9**.

"**Acceptance Tests**" means such tests as may be conducted in as described in **Section 9** and any applicable Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 18**.

"**Approved Third Party Components**" means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor's Bid Response or as part of the State's Security Accreditation Process defined in Schedule E – Data Security Requirements.

"**Authorized Users**" means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

"**Business Day**" means a day other than a Saturday, Sunday or other day on which the State is authorized or required by law to be closed for business.

"**Business Requirements Specification**" means the initial specification setting forth the State's business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

"Contract Change" has the meaning set forth in **Subsection 2.2.**

"Change Notice" means a writing executed by the parties to the Contract memorializing a change to the Contract.

"Change Proposal" has the meaning set forth in **Subsection 2.2.**

"Change Request" has the meaning set forth in **Subsection 2.2.**

"Confidential Information" has the meaning set forth in **Subsection 22.1.**

"**Configuration**" means State-specific changes made to the Software without Source Code or structural data model changes occurring.

"**Contract**" has the meaning set forth in the preamble.

"**Contract Administrator**" is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party's Contract Administrator will be identified in Schedule A or subsequent Change Notices.

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor's Bid Response**" means the Contractor's proposal submitted in response to the Request for Solution.

"**Contractor Hosted**" means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

"**Contractor Personnel**" means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

"**Contractor Project Manager**" means the individual appointed by Contractor and identified in Schedule A or subsequent Change Notices to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

"**Customization**" means State-specific changes to the Software's underlying Source Code or structural data model changes.

"**Deliverables**" means the Software, Services, Documentation, any Hardware, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

"**Deposit Material**" refers to material required to be deposited pursuant to **Section 28.**

"Disaster Recovery Plan" refers to the set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations and to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives.

"**Documentation**" means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Deliverable.

"**DTMB**" means the Michigan Department of Technology, Management and Budget.

"**Effective Date**" has the meaning set forth in the preamble.

"**Fees**" means the fees set forth in the Pricing Schedule attached as **Schedule B**.

"**Financial Audit Period**" has the meaning set forth in **Subsection 23.1.**

"Hardware" means all computer hardware or other equipment provided by Contractor under this Contract, if any, including but not limited to any related accessories.

"**Harmful Code**" means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (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.

"**Hosted Services**" means the hosting, management and operation of the 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.

"**Implementation Plan**" means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

"Integration Testing" has the meaning set forth in **Section 9.**

"**Intellectual Property Rights**" means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in the Contract.

"**Loss or Losses**" means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"**Maintenance Release**" means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections,

enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

"**Milestone**" means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

"**Milestone Date**" means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

"**New Version**" means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

"**Nonconformity**" or **"Nonconformities"** means any failure or failures of a Deliverable, to conform to the requirements of this Contract.

"**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, as set forth in a Statement of Work, 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.

"**Permitted Subcontractor**" means any third party hired by Contractor to perform Services for the State under this Contract, have access to or have the ability to control access to State Data.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"**Pricing Schedule**" means the schedule attached as **Schedule B.**

"Process" means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **"Processing"** and **"Processed"** have correlative meanings.

“**Representatives**” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**RFP**” means the State’s request for proposal designed to solicit responses for Services under this Contract.

“**Services**” means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

“**Service Level Agreement**” means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

“**Site**” means any physical location(s) designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Deliverable, if applicable.

“**Software**” means Contractor’s software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

“**Source Code**” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

“**Specifications**” means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, Request for Solution or Contractor’s Bid Response, if any, for such Software, or elsewhere in a Statement of Work.

“**State**” means the State of Michigan.

“**State Data**” has the meaning set forth in **Section 21.**

“**State Hosted**” means the Hosted Services are not provided by Contractor or one or more of its Permitted Subcontractors.

“**State Materials**” means all materials and information, including but not limited to documents, data, know-how, ideas, methodologies, specifications, software, hardware, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“State Program Managers” are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Deliverables; and (c) perform other duties as may be specified in a Statement of Work. Program Managers will be identified in Schedule A or subsequent Change Notices.

“State Systems” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“**Statement of Work**” means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

“**Stop Work Order**” has the meaning set forth in **Section 15.**

“**Support Services**” means the maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

“System” has the meaning set forth in **Schedule I**.

“System Acceptance” has the meaning set forth in **Schedule I**.

“System Integration Testing” has the meaning set forth in **Schedule I**.

“**Technical Specification**” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

“**Term**” has the meaning set forth in the preamble.

“**Testing Period**” has the meaning set forth in **Section 9.**

“**Transition Period**” has the meaning set forth in **Section 16.**

“**Transition Responsibilities**” has the meaning set forth in **Section 16.**

“**Unauthorized Removal**” has the meaning set forth in **Subsection 2.5.**

“**Unauthorized Removal Credit**” has the meaning set forth in **Subsection 2.5.**

“**User Data**” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input without the inclusion of user derived Information or additional user input.

“**Warranty Period**” means the 90 calendar-day period commencing on the date of the State's Acceptance of the Software or System (if Contractor is providing Hardware under this Contract) for which Support Services are provided free of charge.

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

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor. Contractor will provide Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16.** Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Contract generally or any Statement of Work, including changes to the Services and Implementation Plan (each, a "**Contract Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this Section**.**

(a) As soon as reasonably practicable, and in any case within 20 Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;

(iii) any additional State Resources Contractor deems necessary to carry out such Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within 30 Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's

approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, each parties' Contractor Administrator will sign a Change Notice**.**,

(c) However, if the parties fail to enter into a Change Notice within 15 Business Days following the State's response to a Change Proposal, the State may, in its discretion:

(i) require Contractor to perform or provide the Deliverables under the existing Statement of Work without the Change;

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Subsection 16.1**.

(d) No Change will be effective until the parties have executed a Change Notice. Notwithstanding the foregoing, no Statement of Work or Change Notice executed after the Effective Date will construed to amend or modify this Contract in any way, unless it specifically states its intent to do so and cites the section or sections amended. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e)The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Nonconformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(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; and

(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks. 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.

(c) 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.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor.

(a) Contractor Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

(c) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Upon the occurrence of any event set forth in **Subsections 2.4(c)(i-iii)** above, Contractor will promptly replace its Contractor Project Manager**.** Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 16**, Contractor will issue to the State an amount equal to $25,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to

provide Services to the State under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name the State a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

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

If to State:	If to Contractor:
Jarrod Barron 320 S. Walnut Lansing, MI 48933 BarronJ1@michigan.gov 517-249-0406	Jim Loznak 5555 Corporate Exchange Ct. Grand Rapids,MI 49512 Jim.Loznak@trace3.com 616-337-1057

4. Insurance. Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

5. Software License.

5.1 License terms for the Software is set forth in **Schedule H.**

5.2 **State License Grant to Contractor**. The State hereby grants to Contractor a limited, non-exclusive, non- transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work**.** Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

6. Third Party Components. At least 30 days prior to adding new Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

7. Intellectual Property Rights

7.1 Ownership Rights in Software

(a) For purposes of this **Section 7** only, the term "Software" does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Subsection 7.1(c):**

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide

the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies the State in writing that the Hosted Services are ready for use in a production environment, Acceptance Tests will be conducted as set forth in this **Section 9** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by the State of the notification referenced in **Subsection 9.1(a)**, and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, the State, provided that:

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

9.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in this **Section**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Nonconformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within 10 Business Days, correct such Nonconformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 15 Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Nonconformity in the tested Software.

(a) If such notice is provided by either party and identifies any Nonconformities, the parties' rights, remedies, and obligations will be as set forth in **Subsection 9.4** and **Subsection 9.5.**

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Nonconformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have 30 Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Nonconformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Nonconformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Subsection 9.4** and **Subsection 9.5**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

9.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Nonconformities and re-deliver the Software, in accordance with the requirements set forth in the Contract. Redelivery will occur as promptly as commercially possible and, in any case, within 30 Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Subsection 9. (a)** or **(c)(i)**, identifying any Nonconformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Nonconformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 9**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract in accordance with **Section 16**.

9.6 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Subsection 9.3(b)**, or **(c)(ii)**. Acceptance of the Software may be conditioned upon System Acceptance, if Contractor is providing Hardware, under the terms of this Contract.

10. Non-Software Acceptance.

10.1 If Contractor is providing Hardware under this Contract, Contractor will comply with the requirements for delivery, acceptance and warranty of Hardware as set forth in **Schedule G**.

10.2 System Acceptance. If Contractor is providing Hardware under this Contract, Contractor will comply with the requirements for acceptance testing of the Software and Hardware together as a System, as set forth in **Schedule I**.

10.3 All other non-Software Deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("State Review Period"), unless otherwise provided in the Statement of Work. If the non-Software Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the non-Software Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.**

10.4 Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any non-Software Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable non-Software Deliverables to the State. If acceptance with deficiencies or rejection of the non-Software Deliverables impacts the content or delivery of other non-completed non-Software Deliverables, 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.

10.5 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 provide the non-Software Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

11. Assignment. Contractor may not assign this Contract or any of its rights or delegate any of its duties or obligations hereunder, voluntarily, or involuntarily, whether by merger (regardless of whether it is the surviving or disappearing entity), conversion, consolidation, dissolution, or operation of law to any other party without the prior written 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 governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. 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.

12. Change of Control. Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, 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.

13. Invoices and Payment.

13.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Deliverables. 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.

13.3 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.

13.4 Right of Setoff. 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.

13.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees 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.

13.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any commercial or government customer (including any public educational institution within the State of Michigan) of

Contractor. If Contractor enters into any arrangements with another customer of Contractor to provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify the State of such Fee and formally memorialize the new pricing in a Change Notice.

14. Liquidated Damages.

14.1The parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

14.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. 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 not pay for activities that have been suspended, Contractor's lost profits, or any additional compensation during a stop work period.

16. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

16.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:

i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;

(ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or

(iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If the State terminates this Contract under this **Subsection 16.1**, the State will issue a termination notice specifying whether Contractor must:

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this 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 **Subsection 16.2**.

(c) The State will only pay for amounts due to Contractor for Services 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. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. 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 Services from other sources.

16.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason or no reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(b) continue to perform in accordance with **Subsection 16.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 Transition Responsibilities.

(a) 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; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:

(i) continuing to perform the Services at the established Contract rates;

(ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee;

(iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22**, including without limitation, the return or destruction of State Data at the conclusion of the Transition Period; and

(iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

17. Indemnification

17.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

(a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and

(d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

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

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; and to

(d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior 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. Any litigation activity on behalf of the State or any of its subdivisions 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.

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

18. Infringement Remedies.

18.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

18.2 If any Deliverable, or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(a) procure for the State the right to continue to use such Deliverable, or component thereof to the full extent contemplated by this Contract; or

(b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Deliverable and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Deliverable provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to 6 months to allow the State to replace the affected features of the Deliverable without disruption.

18.4 If Contractor directs the State to cease using any Deliverable under **Subsection 18.3,** the State, at its sole discretion, will be entitled to declare such a direction from the Contractor to cease use a material breach of the Contract and may terminate this Contract under **Section 16**. Unless the claim arose against the Deliverable independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

(a) Contractor's compliance with any designs, specifications, or instructions of the State; or

(b) modification of the Deliverable by the State without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

19.1 The State's Disclaimer of Damages. THE STATE WILL NOT 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, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

19.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR 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 MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

19.3 Contractor's Limitation of Liability. IN NO EVENT WILL CONTRACTOR'S LIABILITY TO THE STATE EXCEED TWO AND A HALF TIMES (2.5X) THE FEES PAYABLE UNDER THIS CONTRACT. THE FOREGOING LIMITATION SHALL NOT APPLY TO CONTRACTOR'S INDEMNIFICATION OBLIGATIONS UNDER THE CONTRACT OR TO CLAIMS FOR INFRINGEMENT OF A U.S. PATENT, COPYRIGHT, TRADEMARK OR TRADE SECRET OR TO CLAIMS FOR DEATH, BODILY INJURY OR TANGIBLE PROPERTY DAMAGE CAUSED BY THE GROSSLY NEGLIGENT OR MORE CULPABLE ACT OR OMISSION OF CONTRACTOR, OR TO CONTRACTOR'S STATE DATA OBLIGATIONS UNDER THE CONTRACT.

20. 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 Permitted Subcontractor, or an officer or director of Contractor or Permitted 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:

(i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or

(ii) 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.

21. State Data.

21.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes:

(a) User Data; and

(b) any other data collected, used, Processed, stored, or generated in connection with the Services, including but not limited to:

(i) personally identifiable information ("**PII**") collected, used, Processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and

(ii) protected health information ("**PHI**") collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

21.2 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.

21.3 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. 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 Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;

(c) keep and maintain State Data in the continental United States and

(d) not use, sell, rent, transfer, mine, distribute, commercially exploit, 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. Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

21.4 Third-Party Requests. Contractor will immediately notify the State upon receipt of any third-party requests which in any way might reasonably require access to State Data. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. Contractor must provide such notification within twenty-four (24) hours from Contractor's receipt of the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State. Upon request by the State, Contractor must provide to the State, its proposed response to the third-party request with adequate time for the State to review, and, as it deems necessary, to revise the response, object, or take other action.

21.5 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 is suspected to compromise the security, confidentiality, integrity, or availability of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable:

(a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;

(b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;

(c) in the case of PII or PHI, at the State's sole election:

(i) 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, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or

(ii) reimburse the State for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) 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 recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and

(i) provide to the State a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, 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. 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, must be reviewed and approved by the State in writing prior to its dissemination.

21.6 The parties agree that any damages arising out of a breach of the terms set forth in this **Section** are to be considered direct damages and not consequential damages.

22. 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.

22.1 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). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

22.2 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 the Contractor’s subcontractor is permissible where:

(a) the subcontractor is a Permitted Subcontractor;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and

(c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State’s Confidential Information in confidence. At the State’s request, any of the Contractor’s and Permitted Subcontractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Subsection 22.2**.

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

22.4 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.

22.5 Surrender of Confidential Information. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 5 Business Days from the date of termination or expiration, return to the other party any and all Confidential Information received from

the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, 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 sanitization methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 5 Business Days from the date of confirmation from the State.

23. Records Maintenance, Inspection, Examination, and Audit.

23.1 Right of Audit. Pursuant to MCL 18.1470, 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 this Contract through the Term of this Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. 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 Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If 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 this Contract must be paid or refunded within 45 calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

24. Support Services. Contractor will provide the State with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Such Support Services will be provided:

(a) Free of charge during the Warranty Period.

(b) Thereafter, for so long as the State elects to receive Support, in consideration of the State's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

25. Data Security Requirements. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will 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's Confidential Information that comply with the requirements of the State's data security policies as set forth in **Schedule E** to this Contract.

26. Training. Contractor will provide, at no additional charge, training on the Deliverable provided hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other

additional training on the Deliverables for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions

27.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State will have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

27.4 Supported Third Party and Open-Source Components. Contractor will utilize only currently supported versions of all Third Party or Open-Source Components and will notify the State when not using the most recently published Third Party and Open-Source Components.

28. Source Code Escrow

28.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. The cost of the escrow will be the sole responsibility of Contractor.

28.2 Deposit. Within 30 business days of the Effective Date, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the Software, Contractor will deposit updated Source Code, documentation, names, and contact information with the escrow agent (all of which is collectively referred to herein as **"Deposit Material"**).

28.3 Verification. At State's request and expense, the escrow agent may at any time verify the Deposit Material, including without limitation by compiling Source Code, comparing it to the Software, and reviewing the completeness and accuracy of any and all material. In the event that the Deposit Material does not conform to the requirements of **Subsection 28.2** above:

(a) Contractor will promptly deposit conforming Deposit Material; and

(b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28** will constitute material breach of this Contract, and no further payments will be due from the State until such breach is cured, in addition to any other remedies the State may have.

28.4 Deposit Material License. Contractor hereby grants the State a license to use, reproduce, and create derivative works from the Deposit Material, provided the State may not distribute or sublicense the Deposit Material or make any use of it whatsoever except for such internal or governmental uses as necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and the State receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 22** (Non-disclosure of Confidential Information) of this Contract (provided no provision of **Subsection 22.4** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

29. Contractor Representations and Warranties.

29.1 Authority. Contractor represents and warrants to the State that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and

(d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.

(e) 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.

29.2 Bid Response. Contractor represents and warrants to the State that:

(a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder to the Request for Solution, and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous 5 years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

29.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) Contractor is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) Contractor has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) Contractor has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(d) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(e) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

(i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable law;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

(i) Harmful Code; or

(ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.

(h) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(i) Contractor will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar

services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;

(k) 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;

(l) 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.

(m) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.

(n) If Contractor Hosted:

(i) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(ii) the Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement;

(iii) all 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 Hosted Services in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Hosted Services have any material undocumented feature;

(o) 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 or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. 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.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

30. 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

including an offer of employment; 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 Permitted Subcontractor that provides Deliverables in connection with this Contract.

31. Compliance with Laws. Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

32. 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, 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 the Contract.

33. Unfair Labor Practice. Under MCL 423.324, the State may void this Contract if the name of the Contractor, or the name of a subcontractor, manufacturer, or supplier of the Contractor, subsequently appears on the Unfair Labor Practice register compiled under MCL 423.322.

34. 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 the Michigan Court of Claims. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

35. Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

36. Force Majeure

36.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

36.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to

Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of 5 Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

36.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Hosted Services or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Hosted Services; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

(b) no Force Majeure Event modifies or excuses Contractor's obligations under **Section 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, Availability Requirement (if Contractor Hosted) defined in the Service Level Agreement, or any data retention or security requirements under the Contract.

37. 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.

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

39. 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.

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

41. Survival. Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification;

disclaimer of damages and limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

42. Administrative Fee and Reporting Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract for transactions with MiDEAL members and other states (including governmental subdivisions and authorized entities). For clarity, Contractor will not be obligated to pay an additional 1% administrative fee for payments made to the Contractor under the Contract for transactions with the State itself. Administrative fee payments must be made online by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee.

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 and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

43. Extended Purchasing Program. This contract 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.

Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

If extended, Contractor must supply all Contract Activities 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.

44. Contract Modification. This Contract may not be amended or modified in any way, except by a properly signed **Change Notice**. Notwithstanding the foregoing, no subsequent Statement of Work or 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.

45. HIPAA Compliance. The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

46. Accessibility Requirements.

46.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to the State, including the level of conformance provided in any PAT. Throughout the Term of the Contract, Contractor must:

(a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;

(b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;

(c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to WCAG 2.0 Level AA;

(d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;

(e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and

(f) participate in the State of Michigan Digital Standards Review described below.

46.2 State of Michigan Digital Standards Review. Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to validate Contractor's accessibility and compliance with WCAG 2.0 Level AA. Prior to the solution going-live and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

46.3 Warranty. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Subsection 16.1**.

46.4 Contractor must, 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 arising out of its failure to comply with the foregoing accessibility standards

46.5 Failure to comply with the requirements in this **Section 47** shall constitute a material breach of this Contract.

47. Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

48. Relationship of the Parties. The relationship between the parties is that of independent contractors. 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. Neither party has authority to contract for nor bind the other party in any manner whatsoever.

49. Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

50. No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

51. Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

52. Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

53. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule
Schedule C	Insurance Schedule
Schedule D	Service Level Agreement

Schedule E	Data Security Requirements
Schedule F	Hardware
Schedule G	System Acceptance Testing
Schedule H	Cisco End User License Agreement

54. Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

55. Entire Agreement. These Terms and Conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the "Contract") constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the Terms and Conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these Terms and Conditions and (b) second, Schedule E – Data Security Requirements and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract. NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE'S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A – STATEMENT OF WORK

1. PURPOSE

Contractor will provide to the State a State-Hosted Cisco Secure Firewall and Intrusion Prevention System (IPS) hardware and software solution consisting of the Cisco products and services listed in **Schedule B** and applicable Services. Contractor will deliver the hardware, software and applicable licensing to enable the State to implement the solution. Contractor will work with the State to ensure the solution is tested and fully implemented no later than May 1, 2024.

2. IT ENVIRONVIRONMENT RESPONSIBILITIES

Definitions For a State Hosted Software Solution:

- **Application** – Software programs which provide functionality for end user and Contractor services.
- **Development** - Process of creating, testing and maintaining software components.

Component Matrix	Name all contractor(s) and/or subcontractor(s) providing each contract component
Application	Cisco for the hardware and software on the firewall
Development	Cisco does create, test and maintain software before releasing to customers. State can develop its own process for updating these firewalls with a test firewall if desired and purchased

3. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

4. USER TYPE AND CAPACITY

The solution must be able to be used by up to 10 State employees and contracted staff resources concurrently.

5. ACCESS CONTROL AND AUTHENTICATION

The Contractor's solution must implement identity federation with the State's MiLogin IT Identity and Access Management (IAM) environment as described in the State of Michigan Administrative Guide (1340.00.020.08 Enterprise Identity and Access Management Services Standard (michigan.gov) .
To support federation with the SOM MILogin solution, the Contractor's solution must support SAML, OpenID or OAuth federated identity protocols. Solutions running within the States internally managed IT environment may be suitable for integration with the State's Active Directory services as identified in the 1340.00.020.08 standard.

6. DATA RETENTION AND REMOVAL

The solution must allow the State to retain all data for the entire length of the Contract. The solution must allow the State to delete data, even data that may be stored off-line or in backups. The solution must allow the State to retrieve data, even data that may be stored off-line or in backups.

7. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes currently supported versions of X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, enterprise storage, monitoring, and management running in house and in cloud hosting provides.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plug-ins or extensions. The rules used to base the minimum browser requirements include:

- Over 2% of desktop and mobile & tablet site traffic, measured using Michigan.gov sessions statistics and
- The current browser identified and approved as the State of Michigan standard

This information can be found at https://www.michigan.gov/browserstats. Please use the most recent calendar quarter to determine browser statistics. Support is required for those desktop and mobile & tablet browsers identified as having over 2% of site traffic.

Contractor must support the current and future State standard environment at no additional cost to the State.

8. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet.**

Contractor must provide a list of any third party components, and open source component included with or used in connection with the deliverables defined within this Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

Look and Feel Standards

All software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at https://www.michigan.gov/standards.

Mobile Responsiveness

If the software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

9. INTEGRATION

Integration services are not needed at this time.

10. MIGRATION

The solution must enable the State to migrate its policy from the existing IPS to the new solution (e.g., blocks configured on the existing system).

11. HARDWARE

Contractor will provide the Hardware listed in **Schedule B**. The State plans to obtain title or ownership of the Hardware.

12. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency. Training may be delivered in a classroom, online or both.

13. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software. Contractor must develop and submit for State approval complete, accurate, and timely solution documentation to support all users, and will update any discrepancies, or errors through the life of the contract. The Contractor's user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

14. CONTRACTOR PERSONNEL

Contractor Contract Administrator. Contractor resource who is responsible to(a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Tammie Buehler 5555 Corporate Exchange Grand Rapids, MI 616-901-9509 tammie.buehler@trace3.com

Contractor Security Officer. Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor's solution. This person must have sufficient knowledge of the security of the Contractor solution and the authority to act on behalf of Contractor in matters pertaining thereto. Contractor must inform the State of any change to this resource.

Contractor
Jim Hunter 5555 Corporate Exchange Grand Rapids, MI 248-425-8623 jim.hunter@trace3.com

Contractor Project Manager. Contractor resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Marisa Miller 678-780-4959 marisa.miller@trace3.com

15. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Contractor must present certifications evidencing satisfactory ICHAT and drug test results for all staff identified for assignment to this project to the State of Michigan Program Manager designated for this Contract. In addition, proposed Contractor personnel will be required to complete a Michigan State Police background check and/or submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC), if required by project.

Annually, Contractor must perform an ICHAT for all staff identified for assignment to this project. Annual background check results will be reported to the State of Michigan Program Manager designated for this Contract.

Contractor, while employed with DTMB, will disclose to the State of Michigan Program Manager for this Contract, in writing at or before the beginning of the next scheduled duty shift:

a. A felony or misdemeanor court conviction, whether by guilty plea, no contest plea or trial.
b. A felony arraignment.
c. Restriction, suspension, or loss of driving privileges for any reason, if the employee's current position requires possession of a valid driver's license.

Contractor will pay for all costs associated with ensuring its staff meet all requirements.

Contractor must notify the State Program Manager(s) prior to removing or replacing any Contractor Personnel with access to State Data under this Contract. Contractor must also provide written certification to the State Program Manager(s) that Contractor Personnel's access to State Data has been terminated. Contractor must notify the State in advance of allocating Contractor Personnel to multiple State Contracts or Projects (discuss timeframe for notification). Contractor must provide detail of how a given Contractor Personnel meets the resource experience requirements in advance of replacing a Contractor Personnel. Contractor must provide monthly summary of Contractor Personnel allocation for all Contractor Personnel who have access to State Data.

Contractor must seek approval from the State prior to removing or replacing any Contractor Personnel with access to State Data.

Offshore Resources. Use of Offshore Resources is prohibited per **Schedule E – Data Security Requirements**. Contractor must comply with the data security and other requirements in this Contract.

Subcontractors. Contractor intends to utilize the following Subcontractor:

The legal business name, address, telephone number of the subcontractor(s).	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95314
A description of subcontractor's organization and the services it will provide and information concerning subcontractor's ability to provide the Contract Activities.	Develop, maintain and support the hardware and software products and associated services listed in **Schedule B** in accordance with end user license agreement in **Schedule H**.

16. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator
Jarrod Barron 517-249-0406 BarronJ1@michigan.gov

Program Managers. The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

DTMB & Agency Program Manager
Aaron Dupre 517-243-9091 DupreA@michigan.gov

17. MEETINGS

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State's Project Manager and the identified State resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, Contractor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

18. PROJECT CONTROL & REPORTS

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State's Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period
- Indicate the number of hours expended during the past week, and the cumulative total to date for the project. Also, state whether the remaining hours are sufficient to complete the project
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified
- Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

All Contractors must submit and enter weekly timesheets into the State of Michigan's Project Portfolio Management tool, Clarity PPM, for approval and reporting. The weekly Clarity PPM timesheet will contain hours worked for assigned project tasks.

19. ADDITIONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A, TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

The Business Specifications Worksheet contains columns and is defined as follows:

Column A: Business Specification number.
Column B: Business Specification description.
Column C: Contractor must indicate how it will comply with the business Specification. Contractor must enter **"Y"** to one of the following:

- **Current Capability –** This capability is available in the proposed solution with no additional configuration or cost.
- **Requires Configuration –** This capability can be met through Contractor-supported changes to existing settings and application options as part of the initial implementation at no additional cost (e.g., setting naming conventions, creating user-defined fields).
- **Customizations to Software Required** – The requirement can be met through Contractor modifying the underlying source code, which can be completed as part of the implementation.
- **Future Enhancement –** This capability is a planned enhancement to the base software and will be available within the next 12 months of contract execution at no additional cost.
- **Not Available –** This capability is not currently available, and a future enhancement is not planned.

NOTE: Configuration is referred to as a change to the solution that must be completed by the awarded Contractor prior to Go-Live but allows an IT or non-IT end user to maintain or modify thereafter (i.e., no source code or structural data model changes occurring).

Customization is referred to a modification to the solution's underlying source code, which can be completed as part of the initial implementation. All configuration changes or customization modifications made during the term of the awarded contract must be forward-compatible with future releases and be fully supported by the awarded Contractor without additional costs.

Contractor shall understand that customizations (i.e., changes made to the underlying source code of the solution) may not be considered and may impact the evaluation of the Contractor's proposal.

Column D: The Contractor must also fully disclose how they will meet the requirements in their proposal response. This column is for Contractor to describe how they will deliver the business Specification and if the Contractor proposes configurations or customizations, the Contractor must explain the details of the impacted risk that may be caused if configured or customized to meet the business Specification. Description must be no more than 250 words for each business Specification.

A	B	C					D
Business Specification Number	**Business Specification**	**Current Capability**	**Requires Configuration**	**Requires Customization**	**Future Enhancement**	**Not Available**	**Contractor must explain how it will deliver the business specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.**
1.0	Ability to implement State Geolocation policy.	Y					Geolocation is easily configurable with an Access Control Rule. It is simple to deploy.
2.0	Ability to add/remove/update IP and URL blocklists as required.	Y					The Cisco Threat Intelligence Director feature of the Firewall Management Center (FMC) supports the import of many threat intelligence feeds. A primary benefit of this feature, is that is aggregates and deduplicates across all 3rd party intelligence feeds.
3.0	Ability to import custom/3rd party IPS rules.	Y					Supported and configurable in the FMC.
4.0	RADIUS based authentication compatible with RSA SecurID	Y					The FMC supports many RADIUS authentications, including RSA.
5.0	Profile endpoints to support asset identification and collection of security posture.	Y					This is configured in the Network Discovery Policy. In addition, the vulnerability info collected within the host profile can be used to auto tune IPS rule sets.
6.0	Ability to capture traffic related to security events that existing packet capture system may not see.	Y					A capture occurs with every IPS event, and with on box decryption included in proposed box, even more information is visible.
7.0	Logs need to include sufficient detail of why packet was dropped.	Y					System identifies reason for block/drop packets, including access controls rules and IPS events which are visible in our Unified Event View. In addition, the Encrypted Visibility Engine (which is included in the proposed solution, but not currently in use at State of Michigan) provides visibility and insight into encrypted traffic flowing thru IPS without needing decryption.
8.0	Solution has appliances for Azure, Google, and AWS clouds.	Y					Cisco supports multiple deployment options for the cloud with centralized management with FMC. This allows a single policy to be deployed in a Hybrid Cloud model, along with sharing of threat intelligence.

SCHEDULE B - PRICING

Part Number	Description	Service Duration (Months)	Qty	Unit Net Price	Extended Net Price
FPR3140-NGFW-K9	Cisco Secure Firewall 3140 NGFW Appliance, 1U		8	$36,984.00	$295,872.00
CON-SNT-FPR3140N	SNTC-8X5XNBD Cisco Secure Firewall 3140 NGFW Applianc	36	8	$19,803.00	$158,424.00
FPR3140T-TMC	Cisco Secure Firewall 3140 TD, Malware and URL License		8	$0.00	$0.00
L-FPR3140T-TMC-3Y	Cisco Secure Firewall 3140 TD, AMP & URL Filtering 3Y Subs	36	8	$56,585.52	$452,684.16
FPR3K-PWR-AC-400	Cisco Secure Firewall 3K Series 400W AC Power Supply		8	$0.00	$0.00
FPR3K-PWR-AC-400	Cisco Secure Firewall 3K Series 400W AC Power Supply		8	$0.00	$0.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m		16	$0.00	$0.00
SF-F3K-TD7.2.3-K9	Cisco Secure Firewall TD 7.2.3 SW for 3100 series appliances		8	$0.00	$0.00
FPR3K-SSD900	Cisco Secure Firewall 3K Series 900GB		8	$0.00	$0.00
FPR3K-SLIDE-RAILS	Cisco Secure Firewall 3100 Slide Rail Kit		8	$0.00	$0.00
FPR3140-BSE	Cisco Secure Firewall 3140 Base Lic		8	$0.00	$0.00
FPR3K-FAN	Cisco Secure Firewall 3K Series Fan Tray		16	$0.00	$0.00
FPR3K-SSD-BLANK	Cisco Secure Firewall 3100 Series SSD Blank Slot Cover		8	$0.00	$0.00
FPR3K-XNM-4X40G	Cisco Secure Firewall 3100 4X40G QSFP+ Netmod		8	$31,226.21	$249,809.68
CON-SNT-FPR40KXN	SNTC-8X5XNBD Cisco FPR3K 4-port 40G QSFP Netmod	36	8	$16,212.63	$129,701.04
FMC4700-K9	Cisco Secure Firewall Management Center 4700 Chassis		1	$64,259.96	$64,259.96
CON-SNT-FMC4700K	SNTC-8X5XNBD Cisco Secure Firewall Management Center	36	1	$51,612.64	$51,612.64
FMC-M6-PS-AC-1050W	Cisco FMC 1050W AC Power Supply		2	$0.00	$0.00
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America		2	$0.00	$0.00
SF-FMC-7.4.0-K9	Cisco Secure Firewall Management Center Software v7.4.0		1	$0.00	$0.00
FMC-M6-P-I8D25GF	Cisco FMC Intel E810XXVDA2 2x25/10 GbE SFP28 PCIe NIC		1	$0.00	$0.00
SFP-10G-SR	10GBASE-SR SFP Module		2	$414.98	$829.96
FMC-M6-HDD-240GB	Cisco FMC 240GB SATA M.2		2	$0.00	$0.00
FMC-M6-HWRAID	Cisco FMC M6 Boot optimized M.2 Raid controller		1	$0.00	$0.00
FMC-M6-TPM-2.0	Cisco FMC Trusted Platform Module 2.0		1	$0.00	$0.00
FMC-M6-MEM-X-16GB	Cisco FMC 16GB 16GB RDIMM SRx4 3200 (8Gb)		8	$0.00	$0.00
FMC-M6-MRAID-12G	Cisco FMC 12G Modular RAID controller with 2GB cache		1	$0.00	$0.00
FMC-M6-HDD-1.2TB	Cisco FMC M6 1.2TB 12G SAS 10K RPM SFF HDD		10	$0.00	$0.00
FMC-M6-O-ID10GC	Cisco FMC Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC		1	$0.00	$0.00
FMC-M6-OCP3-KIT	Cisco FMC C2XX OCP 3.0 Interposer W/Mech Assy		1	$0.00	$0.00
FMC-M6-CPU-A7352	Cisco FMC AMD 2.3GHz 7352 155W 24C/128MB Cache DDR4 3200MHz		1	$0.00	$0.00
				Product Subtotal (hardware/software):	**$1,063,455.76**
				Services Subtotal (support):	**$339,737.68**
				Total Price (3-Year TMC):	**$1,403,193.44**

SCHEDULE C – INSURANCE REQUIREMENTS

1. General Requirements. Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against the State for such damages. Failure to maintain required insurance does not limit this waiver.

2. Qualification of Insurers. Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by DTMB Enterprise Risk Management.

3. Primary and Non-Contributory Coverage. All policies for which the State of Michigan is required to be named as an additional insured must be on a primary and non-contributory basis.

4. Claims-Made Coverage. If any required policies provide claims-made coverage, Contractor must:

a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;

b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.

5. Proof of Insurance.

a. Insurance certificates showing evidence of coverage as required herein must be submitted to DTMB-RiskManagement@michigan.gov within 10 days of the contract execution date.

b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.

c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by DTMB Enterprise Risk Management.

d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).

e. The State may require additional proofs of insurance or solvency, including but not limited to policy declarations, policy endorsements, policy schedules, self-insured certification/authorization, and balance sheets.

f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to DTMB Enterprise Risk Management no later than 5 business days following such cancellation or nonrenewal.

6. Subcontractors. Contractor is responsible for ensuring its subcontractors carry and maintain insurance coverage.

7. Limits of Coverage & Specific Endorsements.

Required Limits	Additional Requirements
Commercial General Liability Insurance	

Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Personal & Advertising Injury $2,000,000 Products/Completed Operations $2,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
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 Occurrence $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.

8. Non-Waiver. This Schedule C 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.

SCHEDULE D – SERVICE LEVEL AGREEMENT

IF THE SOFTWARE IS STATE HOSTED, then the following applies:

The parties agree as follows:

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 Contract Terms and Conditions.

"**Contact List**" means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable the State to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

"**Critical Service Error**" has the meaning set forth in the Service Level Table.

"**Error**" means, generally, any failure or error referred to in the Service Level Table.

"**First Line Support**" means the identification, diagnosis and correction of Errors by the State.

"**High Service Error**" has the meaning set forth in the Service Level Table.

"Low Service Error" has the meaning set forth in the Service Level Table.

"**Medium Service Error**" has the meaning set forth in the Service Level Table.

"**Resolve**" and the correlative terms, "**Resolved**", "**Resolving**" and "**Resolution**" each have the meaning set forth in **Subsection 2.4**

"**Service Credit**" has the meaning set forth in **Section 3**

"**Second Line Support**" means the identification, diagnosis and correction of Errors by the provision of (a) telephone and email assistance by a qualified individual on the Contact List and remote application support, or (b) on-site technical support at the State's premises by a qualified individual on the Contact List.

"**Service Levels**" means the defined Error and corresponding required service level responses, response times, Resolutions and Resolution times referred to in the Service Level Table.

"**State Cause**" means any of the following causes of an Error: (a) a State server hardware problem; (b) a desktop/laptop hardware problem; or (c) a State network communication problem.

"**State Systems**" means the State's information technology infrastructure, including the State's computers, software, databases, electronic systems (including database management systems) and networks.

"**Support Hours**" means 24 hours, 7 days a week.

"**Support Period**" means the period of time beginning 90 days after the date the Software has entered full production mode and ending on the date the Contract expires or is terminated.

"**Support Request**" has the meaning set forth in **Subsection 2.2.**

2. Support Services. The State will provide First Line Support prior to making a Service Request for Second Line Support. Contractor shall perform all Second Line Support and other Support Services during the Support Hours throughout the Support Period in accordance with the terms and conditions of this Schedule and the Contract, including the Service Levels and other Contractor obligations set forth in this **Section 2.**

2.1 Support Service Responsibilities. Contractor shall:

(a) provide unlimited telephone support during all Support Hours;

(b) respond to and Resolve all Support Requests in accordance with the Service Levels;

(c) provide unlimited remote Second Line Support to the State during all Support Hours;

(d) provide on-premise Second Line Support to the State if remote Second Line Support will not Resolve the Error; and

(e) provide to the State all such other services as may be necessary or useful to correct an Error or otherwise fulfill the Service Level requirements, including defect repair, programming corrections and remedial programming.

2.2 Support Requests. Once the State has determined that an Error is not the result of a **State Cause**, the State may request Support Services by way of a Support Request. The State shall classify its requests for Error corrections in accordance with the support request classification and definitions of the Service Level Table set forth in **Subsection 2.4** (each a "**Support Request**"). The State shall notify Contractor of each Support Request by e-mail or telephone. The State shall include in each Support Request a description of the reported Error and the time the State first observed the Error.

2.3 State Obligations. The State shall provide the Contractor with each of the following to the extent reasonably necessary to assist Contractor to reproduce operating conditions similar to those present when the State detected the relevant Error and to respond to and Resolve the relevant Support Request:

(i) if not prohibited by the State's security policies, remote access to the State Systems, and if prohibited, direct access at the State's premises;

(ii) output and other data, documents and information, each of which is deemed the State's Confidential Information as defined in the Contract; and

(iii) such other reasonable cooperation and assistance as Contractor may request.

2.4 Service Level Table. As set out in the **"Service Level Table"** below, Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (a) responded to that Support Request, in the case of response time and (b) Resolved that Support Request, in the case of Resolution time. "**Resolve**", "**Resolved**", "**Resolution**" and correlative capitalized terms mean, with respect to any particular Support Request, that

Contractor has corrected the Error that prompted that Support Request and that the State has confirmed such correction and its acceptance of it in writing. Contractor shall respond to and Resolve all Support Requests within the following times based on the State's designation of the severity of the associated Error, subject to the parties' written agreement to revise such designation after Contractor's investigation of the reported Error and consultation with the State:

SERVICE LEVEL TABLE

Support Request Classifi-cation	Definition	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)
Critical Service Error	(a) Issue affecting entire Software system or single critical production function; (b) Software down or operating in materially degraded state; (c) Data integrity at risk; (d) Material financial impact; (e) Widespread access interruptions: or (f) Classified by the state as a Critical Service Error (g) Hardware not operable	Contractor shall acknowledge receipt of a Support Request within thirty (30) minutes.	For Software: Contractor shall Resolve the Support Request as soon as practicable and no later than four (4) hours after Contractor's receipt of the Support Request. For Hardware: Contractor shall Resolve the Support Request as soon as practicable and no later than four (4) hours after Contractor's receipt of the Support Request. If the Contractor Resolves the Support Request by way of a work-around accepted in writing by the State, the support classification assessment will be reduced to a High Service Error.
High Service Error	(a) A Critical Service Error for which the State has received, within the Resolution time for Critical Service Errors, a work-around that the State has accepted in writing; or (b) Primary component failure that materially impairs Software's performance; (c) Data entry or access is materially impaired on a limited basis; or (d) performance issues of severe nature impacting critical processes	Contractor shall acknowledge receipt of a Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around, within twenty-four (24) hours.	Contractor shall Resolve the Support Request as soon as practicable and no later than two (2) Business Days after Contractor's receipt of the Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around.

Support Request Classifi-cation	Definition	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)
Medium Service Error	An isolated or minor Error in the Software that meets any of the following requirements: (a) does not significantly affect Software functionality; (b) can or does impair or disable only certain non-essential Software functions; or (c) does not materially affect the State's use of the Software	Contractor shall acknowledge receipt of the Support Request within two (2) Business Days.	Contractor shall Resolve the Support Request as soon as practicable and no later than ten (10) Business Days after Contractor's receipt of the Support Request.
Low Service Error	Request for assistance, information, or services that are routine in nature.	Contractor shall acknowledge receipt of the Support Request within five (5) Business Days.	If Low Service Error has not been resolved in sixty (60) Business Days the State may resubmit as a Medium Service Error.

2.5 Escalation. If Contractor does not respond to a Support Request within the relevant Service Level response time, the State may escalate the Support Request to the Contractor Project Manager and State Program Managers, or their designees, and then to the parties' respective Contract Administrators.

2.6 Time Extensions. The State may, on a case-by-case basis, agree in writing to a reasonable extension of the Service Level response or Resolution times.

2.7 Contractor Updates. Contractor shall give the State monthly electronic or other written reports and updates of:

(a) the nature and status of its efforts to correct any Error, including a description of the Error and the time of Contractor's response and Resolution;

(b) its Service Level performance, including Service Level response and Resolution times; and

(c) the Service Credits to which the State has become entitled.

3. Service Credits.

3.1 Service Credit Amounts. If the Contractor fails to respond to a Support Request within the applicable Service Level response time or to Resolve a Support Request within the applicable Service Level Resolution time, the State will be entitled to the corresponding service credits specified in the table below ("**Service Credits**"), provided that the relevant Error did not result from a State Cause.

SERVICE CREDIT TABLE

Support Request Classification	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	An amount equal to 5% of the then current monthly Support Fee for each hour by which Contractor's response exceeds the required Response time.	An amount equal to 5% of the then current monthly Support Fee for each hour by which Contractor's Resolution of the Support Request exceeds the required Resolution time.
High Service Error	An amount equal to 3% of the then current monthly Support Fee for each Business Day, and a pro-rated share of such percentage for each part of a Business Day, by which Contractor's response exceeds the required Response time.	An amount equal to 3% of the then current monthly Support Fee for each Business Day, and a pro-rated share of such percentage for each part of a Business Day, by which Contractor's Resolution of the Support Request exceeds the required Resolution time.

3.2 Compensatory Purpose. The parties intend that the Service 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 Support Services would be impossible or very difficult to accurately estimate as of the Effective Date, and that the Service Credits are a reasonable estimate of the anticipated or actual harm that might arise from Contractor's breach of its Service Level obligations.

3.3 Issuance of Service Credits. Contractor shall, for each monthly invoice period, issue to the State, together with Contractor's invoice for such period, a written acknowledgment setting forth all Service Credits to which the State has become entitled during that invoice period. Contractor shall pay the amount of the Service Credit as a debt to the State within fifteen (15) Business Days of issue of the Service 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 Credit from the amount payable by the State to Contractor pursuant to such invoice.

3.4 Additional Remedies for Service Level Failures. Contractor's repeated failure to meet the Service Levels for Resolution of any Critical Service Errors or High Service Errors, or any combination of such Errors, within the applicable Resolution time set out in the Service Level Table will constitute a material breach under the Contract. Without limiting the State's right to receive Service Credits under this **Section**, the State may terminate this Schedule for cause in accordance with terms of the Contract.

4. Hardware. When the Contractor receives calls for repair and/or replacement of Hardware, the Contractor must correct such problems in accordance with the Service Level Table in Section 2.4 above. The Contractor must maintain sufficient inventory of spare equipment to meet the 1 Business Day requirement. Failure to repair or replace the Hardware within this timeframe will result in the assessment of liquidated damages of $100 per day until resolved.

5. Communications. In addition to the mechanisms for giving notice specified in the Contract, unless expressly specified otherwise in this Schedule or the Contract, the parties may use e-mail for communications on any matter referred to herein.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

Cisco Support Level 1-3 support
1 800 553 2447
1 408 526 7209

Trace3 – escalation beyond Level 3
Tammie Buehler 616-901-9509
Jim Hunter 248-425-8623

SCHEDULE E – DATA SECURITY REQUIREMENTS

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 Contract.

"**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.).

"Hosting Provider" means any Permitted 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

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. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at https://www.michigan.gov/dtmb/policies/it-policies.

This responsibility also extends to all service providers and subcontractors 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 Standard. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Standard, see https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013002-Acceptable-Use-of-Information-Technology-Standard.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Standard before accessing State systems or Data. 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 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all 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 either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause.

5.2 for Hosted Services provided by the Contractor, 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.

5.3 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, developed and backed up in the continental United States, and the data center(s) in which State Data resides minimally meets Uptime Institute Tier 3 standards (https://www.uptimeinstitute.com/), or its equivalent;

5.4 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;

5.5 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the System for Award Management (SAM) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

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, consistent with best industry practice and applicable standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.7 take all reasonable measures 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; and (iii) unauthorized access to any of the State Data;

5.8 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.9 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 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

5.11 Contractor must permanently sanitize or destroy the State's information, including State Data, from all media both digital and nondigital including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. Contractor must sanitize information system media, both digital and non-digital, prior to disposal, release out of its control, or release for reuse as specified above.

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within two weeks of the State's request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs, perform related remediation activities, and provide evidence of compliance. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

7. Unauthorized Access. Contractor may not access, and must 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. 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 authorization pursuant to this Section. All State-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 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. 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. If the State chooses to perform an on-site audit, Contractor will, make all such 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 five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; 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. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Hosted Services and their housing facilities and operating environments.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's FedRAMP System Security Plan(s) or SOC 2 Type 2 report(s) to the State within two weeks of the State's request. 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 implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

8.5 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8.**

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 as required by the State Web Application Security Standard and other applicable PSPs.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

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

(a) Contractor must either a) grant the State the right to dynamically scan a deployed version of the Software; or b) in lieu of the State performing the scan, Contractor must dynamically scan a deployed version of the Software using a State approved application scanning tool, and provide the State with a vulnerabilities assessment after Contractor has completed such scan. These scans and assessments i) must be completed and provided to the State quarterly (dates to be provided by the State) and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans.

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

(a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third party and open source software initially, for all updated third party and open source software, and for all third party and open source software in each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans if not provided as part of SAST and/or DAST reporting.

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 ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly and provide the scan’s assessments to the State in a format that is specified by

the State and used to track the remediation. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in the State's PSPs.

11. Nonexclusive Remedy for Security Breach.

11.1 Any failure of the Services to 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, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE F – HARDWARE

1. **Definitions**. All initial capitalized terms in this Schedule that are not defined herein shall have the respective meanings given to them in the Contract.

2. **Hardware**. Contractor must provide fully functioning Hardware that fully integrates with the Software and performs in accordance with the requirements and specifications set forth in the Contract.

3. **Delivery**. Contractor must deliver the Hardware to the locations designated by the State by the delivery date specified in the Statement of Work, or as otherwise specified in writing by the State. Five (5) Business Days prior to the actual delivery date, Contractor must give written notice to the State specifying the precise delivery date and time. Contractor must pay all costs associated with replacing any item damaged in transit to the final destination. Contractor acknowledges that no item will be considered delivered on the delivery date if it is damaged or otherwise not ready for the State to begin its acceptance procedures. Contractor must, at a minimum, package the Hardware according to industry standards and include a packing slip with each shipment. Contractor must also arrange for any rigging and drayage necessary to deliver the Hardware. All costs associated with packaging, shipping, transportation, delivery and insurance are to be borne by Contractor.

4. **Installation, Integration and Configuration.**
   a. Contractor must unpack, assemble, install, integrate, interconnect, configure and otherwise provide and make fully operational all the Hardware at the locations specified by the State prior to the applicable dates in accordance with the criteria set forth by the State. Where necessary to complete installation, Contractor must provide all required moving and installation resources, including but not limited to personnel, packing material, and floor protection panels as necessary. After completing installation, Contractor must provide the State with written notification that the Hardware is ready for use and acceptance.
   b. Contractor must supply all materials required to complete the assembly, installation, integration, interconnection, and configuration of the Hardware at the locations specified by the State so that it is ready for use and acceptance, including providing and setting up all required connections to the power supply and any other necessary cables and any other accessories or supplies.
   c. Contractor must leave all work areas clean once installation is complete, which includes removing and disposing of all packing materials.
   d. Unless otherwise provided for in the Pricing Schedule, all costs associated with the installation services described in this Section are to be borne by Contractor.

5. **Documentation**. Contractor must provide to the State all end-user documentation for the Hardware. The documentation, at a minimum, must include all the documentation available to consumers from the manufacturer of the Hardware about the technical specifications of the Hardware, installation requirements, and operating instructions, as well as details about the software programs with which the Hardware functions.

6. **Acceptance**. This Section applies to the acceptance of the Hardware itself. Acceptance of the Hardware may be conditioned on System Acceptance in Schedule I.
   a. The Hardware is subject to inspection and acceptance by the State. As part of its acceptance process, the State may test any function of the Hardware to determine whether it meets the requirements set forth in this Contract. If the State accepts the Hardware, the State will notify

Contractor in writing. Unless otherwise provided in the Statement of Work, if the Hardware is not fully accepted by the State, the State will notify Contractor in writing that either: (a) the Hardware is accepted but noted deficiencies must be corrected; or (b) the Hardware is rejected. If the State finds material deficiencies, it may: (i) reject the Hardware without performing any further inspections; (ii) demand performance at no additional cost; or (iii) deem such material deficiencies to be a breach of the Contractor's obligations under the terms of the Contract and terminate this Contract in accordance with Section 16.

b. Within 10 Business Days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Hardware, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Hardware to the State. If acceptance with deficiencies or rejection of the Hardware impacts the content or delivery of Deliverables, 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.
c. 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.
d. Acceptance by the State does not relieve Contractor of its responsibility for defects in the Hardware or other failures to meet the requirements of the Contract or of its support and maintenance obligations.

7. **Support and Warranty for Hardware**.
   a. Throughout the Term, Contractor will provide, through its Subcontractor (Cisco), maintenance and support of the Hardware and will repair, service, or replace any defective or nonconforming Hardware in accordance with the requirements set forth in this Contract, including without limitation the Service Level Agreement.
   b. Contractor will provide and assign or otherwise transfer to the State or its designee all applicable manufacturer's warranties regarding all Hardware or as otherwise provided for in the Contract.

8. **Further Representations and Warranties.** Contractor represents and warrants that:
   a. all Hardware is delivered free from any security interest, lien, or encumbrance and will continue in that respect;
   b. the Hardware will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party;
   c. it has the unconditional and irrevocable right, power and authority to provide to the State the Hardware throughout the Term and any additional periods during which Contractor does or is required to provide Hardware to the State; and
   d. Contractor will pass-through any applicable manufacturing warranty.
9. **Risk of Loss and Title**. Title and risk of loss or damage to Hardware remains with Contractor until delivery to the State. 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 Hardware, Contractor must remove the Hardware from the premises within 10 calendar days after notification of rejection. The risk of loss of rejected or nonconforming Hardware remains with Contractor. Contractor must reimburse the State for costs and expenses incurred in storing or effecting removal or disposition of rejected Hardware that the Contractor fails to remove in a timely manner pursuant to this Section. Title passes to the State upon final Acceptance of the Hardware.

SCHEDULE G – SYSTEM ACCEPTANCE

1. Definitions. For purposes of this Schedule I, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in Section 1 have the respective meanings given to them in the Contract.

"**System**" has the meaning set forth in Subsection 2.1(a) of this Schedule.

"**System Acceptance**" has the meaning set forth in Subsection 2.6 of this Schedule.

"**System Acceptance Tests**" means such tests as may be conducted in accordance with this **Schedule** to determine whether the System meets the requirements of this Contract.

"System Integration Testing" has the meaning set forth in Subsection 2.2(a) of this Schedule.

"System Testing Period" has the meaning set forth in Subsection 2.1(b) of this Schedule.

2. System Acceptance Testing.

2.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software and Hardware together (the "**System**"), or upon any changes to such System, System Acceptance Tests will be conducted as set forth in this **Schedule** to ensure the System as a whole conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All System Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following the receipt by the State of written notification that the System is ready to have System Acceptance Tests performed, and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the "**System Testing Period**"). System Acceptance Tests will be conducted by the party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, the State, provided that:

(i) for System Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such System Acceptance Tests; and

(ii) for System Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such System Acceptance Tests.

2.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of System Acceptance Tests.

(a) Upon delivery and installation of any application programming interfaces, applicable Work Product, Configuration or Customizations to the Software, or additions or changes to the Hardware, under a Statement of Work, additional System Acceptance Tests may be performed on the modified System as a whole to ensure full operability, integration, and compatibility among all elements of the System ("**System Integration Testing**"). System Integration Testing is subject to all procedural and other terms and conditions set forth in this Schedule.

(b) The State may suspend System Acceptance Tests and the corresponding System Testing Period by written notice to Contractor if the State discovers a material Nonconformity in the tested System or part or feature of the System. In such event, Contractor will immediately, and in any case within 10 Business Days, correct such Nonconformity, whereupon the System Acceptance Tests and System Testing Period will resume for the balance of the System Testing Period.

2.3 Notices of Completion, Nonconformities, and Acceptance. Within 15 Business Days following the completion of any System Acceptance Tests, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Nonconformity in the tested System.

(a) If such notice is provided by either party and identifies any Nonconformities, the parties' rights, remedies, and obligations will be as set forth in **Subsections 2.4** and **2.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Nonconformities, such notice constitutes the State's acceptance of such System.

(c) If such notice is provided by Contractor and identifies no Nonconformities, the State will have 30 Business Days to use the System in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the System contains no Nonconformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Nonconformities the State has observed in the System and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Subsections 2.4** and **2.5**; or

(ii) provide Contractor with a written notice of its acceptance of such System, which must be signed by the State Program Managers or their designees.

2.4 Failure of Acceptance Tests. If System Acceptance Tests identify any Nonconformities, Contractor, at Contractor's sole cost and expense, will remedy all such Nonconformities and re-deliver the System, or relevant portion thereof, in accordance with the requirements set forth in a Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within 30 Business Days following, as applicable, Contractor's:

(a) completion of such System Acceptance Tests, in the case of System Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Subsections 2.3(a)** or **2.3(c)(i)**, identifying any Nonconformities.

2.5 Repeated Failure of Acceptance Tests. If System Acceptance Tests identify any Nonconformity in the System after a second or subsequent delivery, or Contractor fails to re-deliver the System on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Schedule**;

(b) accept the System as nonconforming, in which case the Fees for the System will be reduced equitably to reflect the value of the System as received relative to the value of the System had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract in accordance with Error! Reference source not found.**Section 16** of the Contract Terms and Conditions.

2.6 System Acceptance. Acceptance of the System ("**System Acceptance**") (subject, where applicable, to the State's right to System Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the System under **Subsection 2.3(b)**, or **2.3(c)(ii)**

SCHEDULE H – CISCO END USER LICENSE AGREEMENT

Cisco End User License Agreement

1. Scope and Applicability

1.1 This End User License Agreement ("**EULA**") between the State of Michigan ("**You**") and Cisco Systems, Inc. ("**Cisco**") covers Your use of the Software and Cloud Services ("**Cisco Technology**") purchased under Cisco Deal ID 74541641. Definitions of capitalized terms are in Section 13 (Definitions).

1.2 **You agree to be bound by this EULA through:**

(a) Your download, installation, or use of the Cisco Technology; or

(b) Your express agreement to this EULA.

1.3 **If You do not have authority to enter into this EULA or You do not agree with its terms, do not use the Cisco Technology. You may request a refund for the Software within 30 days of Your initial purchase provided You return the Software to the Approved Source and disable or uninstall it. This paragraph does not apply where You have expressly agreed to end user license terms with Cisco as part of a transaction with an Approved Source.**

1.4 **Term.** This EULA will be effective from the date of last signature below ("**Effective Date**") and covers Your access to, and use of Cisco Technology You acquire from an Approved Source for a period of three (3) years from the Effective Date.

2. Using Cisco Technology

2.1 **License and Right to Use**. Cisco grants You a non-exclusive, non-transferable (except regarding Software, as permitted under the Cisco Software Transfer and Re-Use Policy):

(a) license to use the Software; and

(b) right to use the Cloud Services

both as acquired from an Approved Source, for Your direct benefit during the Usage Term and as set out in Your Entitlement and this EULA (collectively, the "**Usage Rights**").

2.2 **Use by Third Parties**. You may permit Authorized Third Parties to exercise the Usage Rights on Your behalf, provided that You are responsible for:

(a) ensuring that such Authorized Third Parties comply with this EULA; and

(b) any breach of this EULA by such Authorized Third Parties.

2.3 **Beta and Trial Use**. If Cisco grants You Usage Rights in Cisco Technology on a trial, evaluation, beta or other free-of-charge basis ("**Evaluation Software and Services**"):

(a) You may only use the Evaluation Software and Services on a temporary basis for the period limited by the license key or specified by Cisco in writing. If there is no period identified, such use is limited to 30 days after the Evaluation Software and Services are made available to You;

(b) If You fail to stop using and/or return the Evaluation Software and Services or the equipment on which it is authorized for use by the end of the trial period, You may be invoiced for its list price and agree to pay such invoice;

(c) Cisco, in its discretion, may stop providing the Evaluation Software and Services at any time, at which point You will no longer have access to any related data, information, and files and must immediately cease using the Cisco Technology; and

(d) The Evaluation Software and Services may not have been subject to Cisco's usual testing and quality assurance processes and may contain bugs, errors, or other issues. Unless agreed in writing by Cisco, You will not put Evaluation Software and Services into production use. Cisco provides Evaluation Software and Services "AS-IS" without support or any express or implied warranty or indemnity for any problems or issues, and Cisco has no liability relating to Your use of the Evaluation Software and Services.

2.4 **Upgrades or Additional Copies of Software.** You may only use Upgrades or additional copies of the Software beyond Your license Entitlement if You have:

(a) acquired such rights under a support agreement covering the Software; or

(b) purchased the right to use Upgrades or additional copies separately.

2.5 **Interoperability of Software.** If required by law and upon Your request, Cisco will provide You with the information needed to achieve interoperability between the Software and another independently created program, provided You agree to any additional terms reasonably required by Cisco. You will treat such information as Confidential Information.

2.6 **Subscription Renewal.** Usage Rights in Cisco Technology acquired on a subscription basis will automatically renew for the renewal period indicated on the order You or Your Cisco Partner placed with Cisco ("**Renewal Term**") unless:

(a) You notify Your Approved Source in writing at least 45 days before the end of Your then-current Usage Term of Your intention not to renew; or

(b) You or Your Cisco Partner elect not to auto-renew at the time of the initial order placed with Cisco. Cisco acknowledges that You have elected not to auto-renew.

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 Cisco Partner promptly notify Cisco in writing, before the renewal date, that You do not accept the fee changes. In that case, Your subscription will terminate at the end of the current Usage Term.

3. Additional Conditions of Use

3.1 **Cisco Technology Generally.** Unless expressly agreed by Cisco, You may not:

(a) transfer, sell, sublicense, monetize or make the functionality of any Cisco Technology available to any third party;

(b) use the Software on second hand or refurbished Cisco equipment not authorized by Cisco, or use Software licensed for a specific device on a different device (except as permitted under Cisco's Software License Portability Policy);

(c) remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks;

(d) reverse engineer, decompile, decrypt, disassemble, modify, or make derivative works of the Cisco Technology; or

(e) use Cisco Content other than as part of Your permitted use of the Cisco Technology.

3.2 **Cloud Services.** You will not intentionally:

(a) interfere with other customers' access to, or use of, the Cloud Service, or with its security;

(b) facilitate the attack or disruption of the Cloud Service, including a denial-of-service attack, unauthorized access, penetration testing, crawling or distribution of malware (including viruses, trojan horses, worms, time bombs, spyware, adware and cancelbots);

(c) cause an unusual spike or increase in Your use of the Cloud Service that negatively affects operation of the Cloud Service; or

(d) submit any information that is not contemplated in the applicable Documentation.

3.3 **Evolving Cisco Technology**

(a) **Changes to Cloud Services.** Cisco may:

(1) enhance or refine a Cloud Service, although in doing so, Cisco will not materially reduce the core functionality of that Cloud Service, except as contemplated in Section 3.3(b) (End of Life); and

(2) perform scheduled maintenance of the infrastructure and software used to provide a Cloud Service, during which You may experience some disruption to that Cloud Service. Whenever reasonably practicable, Cisco will provide You with advance notice of such maintenance. You acknowledge that occasionally, Cisco may need to perform emergency maintenance without providing You advance notice, during which Cisco may temporarily suspend Your access to, and use of, the Cloud Service.

(b) **End of Life**

(1) Cisco may end the life of Cisco Technology, including component functionality ("EOL"), by providing written notice on Cisco.com. If You or Your Cisco Partner prepaid a fee for Your use of Cisco Technology that becomes EOL before the expiration of Your then-current Usage

Term, Cisco will use commercially reasonable efforts to transition You to a substantially similar Cisco Technology. If Cisco does not have substantially similar Cisco Technology, then Cisco will credit You or Your Cisco Partner any unused portion of the prepaid fee for the Cisco Technology declared EOL ("EOL Credit").

(2) The EOL Credit will be calculated from the last date the applicable Cisco Technology is available to the last date of the applicable Usage Term. Such credit can be applied towards the future purchase of Cisco products or any open accounts receivable.

3.4 **Protecting Account Access.** You will keep all account information up to date, use reasonable means to protect Your account information, passwords and other login credentials, and promptly notify Cisco of any known or suspected unauthorized use of or access to Your account.

3.5 **Use with Third Party Products.** If You use the Cisco Technology with third party products, such use is at Your risk. You are responsible for complying with any third-party provider terms, including its privacy policy. Cisco does not provide support or guarantee ongoing integration support for products that are not a native part of the Cisco Technology.

3.6 **Open Source Software.** Open source software not owned by Cisco is subject to separate license terms set out at www.cisco.com/go/opensource. Cisco warrants that its use of open source code in Cisco Technology will not:

(a) materially or adversely affect Your ability to exercise Usage Rights in that Cisco Technology; or

(b) cause Your software to become subject to an open source license, provided You only use Cisco Technology in accordance with Documentation and in object code form.

4. Fees

To the extent permitted by law, orders for the Cisco Technology are non-cancellable. Fees for Your use of Cisco Technology are set out in Your purchase terms with Your Cisco Partner. If You use Cisco Technology beyond Your Entitlement ("**Overage**"), Your Cisco Partner may invoice You, and You agree to pay, for such Overage, in accordance with the rates set forth in the purchase terms with Your Cisco Partner.

5. Confidential Information and Use of Data

5.1 **Confidentiality**

(a) Recipient will hold in confidence and use no less than reasonable care to avoid disclosure, except as required by law, of any Confidential Information to any third party, except for its employees, affiliates and contractors who have a need to know ("**Permitted Recipients**").

(b) Recipient:

(1) must ensure that its Permitted Recipients are subject to written confidentiality obligations no less restrictive than the Recipient's obligations under this EULA; and

(2) is liable for any breach of this Section by its Permitted Recipients.

(c) Such nondisclosure obligations will not apply to information which:

(1) is known by Recipient without confidentiality obligations;

(2) is or has become public knowledge through no fault of Recipient; or

(3) is independently developed by Recipient.

(d) Recipient may disclose Discloser's Confidential Information if required under a regulation, law or court order, including but not limited to the Michigan Freedom of Information Act, provided that, except for disclosure required under the Michigan Freedom of Information Act, Recipient provides prior notice to Discloser (to the extent legally permissible) and reasonably cooperates, at Discloser's expense, regarding protective actions pursued by Discloser. Recipient agrees to assert any available exemptions permitted by the Michigan Freedom of Information Act.

(e) Upon the reasonable request of Discloser, Recipient will either return, delete or destroy all Confidential Information of Discloser and certify the same.

5.2 **How We Use Data.**

Cisco will access, process and use data in connection with Your use of the Cisco Technology in accordance with applicable privacy and data protection laws. Cisco's Customer Master Data Protection Agreement ("**Customer MDPA**") which is available at this link (or terms executed between You and Cisco governing the same scope) is incorporated by reference and solely applies to Your personal data as defined in the MDPA processed by Cisco on Your behalf when using the Cisco Technology. For further detail, please visit Cisco's Security and Trust Center. Cisco uses Systems Information, Personal Data and Customer Content

(collectively "Data") as described in the Data Briefs, including the Information Security Data Brief, located at www.cisco.com/go/data.

5.3 **Notice and Consent.** To the extent Your use of the Cisco Technology requires it, You are responsible for providing notice to, and obtaining consents from, individuals regarding the collection, processing, transfer and storage of their data through Your use of the Cisco Technology.

6. Ownership

6.1 Unless agreed in writing, nothing in this EULA transfers ownership in, or grants any license to, any intellectual property rights. You retain any ownership of Your content and Cisco retains ownership of the Cisco Technology and Cisco Content.

6.2 Cisco may use any feedback You provide in connection with Your use of the Cisco Technology as part of its business operations.

7. Indemnification

7.1 **Claims.** Cisco will defend any third party claim against You that Your valid use of Cisco Technology under Your Entitlement infringes a third party's patent, copyright or registered trademark (the "**IP Claim**"). Cisco will indemnify You against the final judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim, provided that You promptly notify Cisco in writing of the IP Claim. You are entitled to the following:

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ Your own counsel; and to

(d) Retain control of the defense, at its own cost and expense, if You deem necessary. Cisco will not, without Your prior 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. Any litigation activity on behalf of You or any of its subdivisions, under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent You may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

Cisco will have no obligation to reimburse You for attorney fees and costs incurred prior to Cisco's receipt of notification of the IP Claim. You, at Your own expense, may retain Your own legal representation.

7.2 **Additional Remedies.** If an IP Claim is made and prevents Your exercise of the Usage Rights, Cisco will either procure for You the right to continue using the Cisco Technology, or replace or modify the Cisco Technology with functionality that is at least equivalent. Only if Cisco determines that these alternatives are not reasonably available, Cisco may terminate Your Usage Rights granted under this EULA upon written notice to You and will refund You a prorated portion of the fee You paid for the Cisco Technology for the remainder of the unexpired Usage Term.

7.3 **Exclusions.** Cisco has no obligation regarding any IP Claim based on:

(a) compliance with any designs, specifications, or requirements You provide or a third party provides;

(b) Your modification of any Cisco Technology or modification by a third party;

(c) the amount or duration of use made of the Cisco Technology, revenue You earned, or services You offered;

(d) combination, operation, or use of the Cisco Technology with non-Cisco products, software or business processes;

(e) Your failure to modify or replace the Cisco Technology as required by Cisco; or

(f) any Cisco Technology provided on a no charge, beta or evaluation basis.

7.4 This Section 7 states Cisco's entire obligation and Your exclusive remedy from Cisco regarding any IP Claim against You.

8. Warranties and Representations

8.1 **Performance.** Cisco warrants that:

(a) for 90 days from the Delivery Date or longer as stated in Documentation, or on www.cisco.com/go/warranty, the Software substantially complies with the Documentation; and

(b) during the Usage Term, it provides the Cloud Services with commercially reasonable skill and care in accordance with the Documentation.

8.2 **Malicious Code.** Cisco warrants that it will use vulnerability detection technologies and practices in accordance with Leading Industry Practice to prevent any Malicious Code being introduced by it in providing the Cisco Technology. "Leading Industry Practice" means the exercise of that skill, care and diligence as would be reasonably expected from a leading provider of services substantially similar to the Cisco Technology.

8.3 **Qualifications**

(a) Sections 8.1 and 8.2 do not apply if the Cisco Technology or the equipment on which it is authorized for use:

(1) has been altered, except by Cisco or its authorized representative;

(2) has been subjected to abnormal physical conditions, accident or negligence, or installation or use inconsistent with this EULA or Cisco's instructions;

(3) is acquired on a no charge, beta or evaluation basis;

(4) is not a Cisco-branded product or service; or

(5) has not been provided by an Approved Source.

(b) Upon Your prompt written notification to the Approved Source during the warranty period of Cisco's breach of this Section 8, Your sole and exclusive remedy (unless otherwise required by law) is, at Cisco's option, either:

(1) repair or replacement of the applicable Cisco Technology; or

(2) a refund of either:

(A) the license fees paid for the non-conforming Software; or

(B) the fees paid for the period in which the Cloud Service did not comply, excluding any amounts paid or owed under an applicable service level agreement/objective.

(c) Where Cisco provides a refund of license fees for Software, You must return or destroy all copies of the applicable Software.

(d) Except as set out in this Section and to the extent permitted by law, Cisco expressly disclaims all warranties and conditions of any kind, express or implied, including without limitation any warranty, condition or other implied term as to merchantability, fitness for a particular purpose or non-infringement, or that the Cisco Technology will be secure, uninterrupted or error-free. This warranty disclaimer is in no way intended to negate Cisco's security and data protection obligations set forth within its Information Security Data Brief.

(e) If You are a consumer, You may have legal rights in Your country of residence that prohibit the limitations set out in this Section from applying to You, and, to the extent prohibited, they will not apply.

9. Liability

9.1 Neither party will be liable for indirect, incidental, exemplary, special or consequential damages; loss or corruption of data or interruption or loss of business; or loss of revenues, profits, goodwill or anticipated sales or savings.

9.2 The maximum aggregate liability of each party under this EULA is limited to:

(a) for claims solely arising from Software licensed on a perpetual basis, the fees received by Cisco for that Software; or

(b) for all other claims, the fees received by Cisco for the applicable Cisco Technology and attributable to the 12 month period immediately preceding the first event giving rise to such liability.

9.3 Sections 9.1 and 9.2 do not apply to liability arising from:

(a) Your failure to pay all amounts due; or

(b) Your breach of Sections 2.1 (License and Right to Use), 3.1 (Cisco Technology Generally), 3.2 (Cloud Services) or 12.8 (Export);

9.4 This limitation of liability applies whether the claims are in warranty, contract, tort (including negligence), infringement, or otherwise, even if either party has been advised of the possibility of such damages. Nothing in this EULA limits or excludes any liability that cannot be limited or excluded under applicable law. This limitation of liability is cumulative and not per incident.

10. Termination and Suspension

10.1 **Suspension**. Cisco may immediately suspend Your Usage Rights if You breach Sections 2.1 (License and Right to Use), 3.1 (Cisco Technology Generally), 3.2 (Cloud Services), 5.1 (Confidentiality) or 12.8 (Export).

10.2 **Termination**

(a) If a party materially breaches this EULA and does not cure that breach within 30 days after receipt of written notice of the breach, the non-breaching party may terminate this EULA for cause.

(b) Cisco may immediately terminate this EULA if You breach Sections 2.1 (License and Right to Use), 3.1 (Cisco Technology Generally), 3.2 (Cloud Services) or 12.8 (Export).

(c) Upon termination of the EULA, You must stop using the Cisco Technology and destroy any copies of Software and Confidential Information within Your control.

(d) If this EULA is terminated due to Cisco's material breach, Cisco will refund You or Your Approved Source, the prorated portion of fees You have prepaid for the Usage Rights beyond the date of termination.

(e) Upon Cisco's termination of this EULA for Your material breach, You will pay Cisco or the Approved Source any unpaid fees through to the end of the then-current Usage Term. If You continue to use or access any Cisco Technology after termination, Cisco or the Approved Source may invoice You, and You agree to pay, for such continued use.

10.3 **Termination of Agreement with Cisco Partner.** This EULA is automatically terminated upon termination of Your agreement with the Cisco Partner.

11. Verification

11.1 During the Usage Term and for a period of 12 months after its expiry or termination, You will take reasonable steps to maintain complete and accurate records of Your use of the Cisco Technology sufficient to verify compliance with this EULA ("**Verification Records**"). Upon reasonable advance notice, and no more than once per 12 month period, You will, within 30 days from Cisco's notice, let Cisco and its auditors who are under a written obligation of confidentiality access to the Verification Records.

11.2 If the verification process discloses underpayment of fees:

(a) Cisco Partner may invoice the State pursuant to the terms of Your agreement with the Cisco Partner

12. General Provisions

12.1 **Survival**. Sections 3 (Additional Conditions of Use), 4 (Fees), 5 (Confidential Information and Use of Data), 6 (Ownership), 8 (Warranties and Representations), 9 (Liability), 10 (Termination and Suspension), 11 (Verification) and 12 (General Provisions) survive termination or expiration of this EULA.

12.2 **Third Party Beneficiaries**. This EULA does not grant any right or cause of action to any third party.

12.3 **Assignment and Subcontracting.**

(a) Except as set out below, neither party may assign or novate this EULA in whole or in part without the other party's express written consent.

(b) Cisco may:

(1) by written notice to You, assign or novate this EULA in whole or in part to an Affiliate of Cisco, or otherwise as part of a sale or transfer of any part of its business, and in any such case, such assignment or novation shall be to an entity of sufficient net worth to meet any potential liability under this Agreement; provided however, that such entity must not be disbarred by the State of Michigan or the federal government and is otherwise not prohibited from doing business in the State of Michigan; or

(2) subcontract any performance associated with the Cisco Technology to third parties, provided that such subcontract does not relieve Cisco of any of its obligations under this EULA.

12.4 **US Government End Users.** The Software, Cloud Services and Documentation are deemed to be "commercial computer software" and "commercial computer software documentation" pursuant to FAR 12.212 and DFARS 227.7202. All US Government end users acquire the Software, Cloud Services and Documentation with only those rights set forth in this EULA. Any provisions that are inconsistent with federal procurement regulations are not enforceable against the US Government.

12.5 **Cisco Partner Transactions.** If You purchase Cisco Technology from a Cisco Partner, the terms of this EULA apply to Your use of that Cisco Technology and prevail over any inconsistent provisions in Your agreement with the Cisco Partner as between You and Cisco only. The terms of this EULA apply independently of any contract You may have with a Cisco partner.

12.6 **Modifications to the EULA**. This EULA, or any of its components, may not be amended or modified in any way, except by a properly signed written agreement by the parties. Changes to the EULA apply to any Entitlements acquired or renewed after the date of modification.

12.7 **Compliance with Laws**

(a) **General.** Each party will comply with all laws and regulations applicable to their respective obligations under this EULA. Cisco may restrict the availability of Cisco Technology in any particular location or modify or discontinue features to comply with applicable laws and regulations.

(b) **Data collection and transfer.** If You use the Cisco Technology in a location with local laws requiring a designated entity to be responsible for collection of data about individual end users and transfer of data outside of that jurisdiction (e.g. Russia and China), You acknowledge that You are the entity responsible for complying with such laws.

12.8 **Export**. Cisco's Software, Cloud Services, products, technology and services (collectively the "**Cisco Products**") are subject to U.S. and local export control and sanctions laws. You acknowledge and agree to the applicability of and Your compliance with those laws, and You will not receive, use, transfer, export or re-export any Cisco Products in a way that would cause Cisco to violate those laws. You also agree to obtain any required licenses or authorizations.

12.9 **Governing Law and Venue.** This EULA, and any disputes arising from it, will be governed exclusively in accordance with Michigan law. Any dispute arising from this EULA must be resolved in Michigan Court of Claims. Cisco consents to venue in Ingham County.

12.10 **Notice**. Any informational notice concerning the Cisco Technology delivered by Cisco to You under this EULA will be delivered via email, regular mail or postings on Cisco.com. Legal notices to Cisco should be sent to Cisco Systems, Office of General Counsel, 170 West Tasman Drive, San Jose, CA 95134 unless this EULA, or an order specifically allows other means of notice. Legal notices to You should be sent to: Jarrod Barron, 320 S. Walnut, Lansing, MI 48933.

12.11 **Force Majeure.** Neither party will be responsible for failure to perform its obligations due to an event or circumstances beyond its reasonable control. In the event the force majeure event precludes the payment of monies due and owing by You, Cisco will continue to perform during the pendency of such event (assuming the Force Majeure event doesn't also preclude such performance by Cisco) and You will pay Cisco Partner for such service retroactively.

12.12 **No Waiver.** Failure by either party to enforce any right under this EULA will not waive that right.

12.13 **Severability.** If any portion of this EULA is not enforceable, it will not affect any other terms.

12.14 **Entire agreement.** This EULA is the complete agreement between the parties regarding the subject matter of this EULA and supersedes all prior or contemporaneous communications, understandings or agreements (whether written or oral).

12.15 **Translations**. Cisco may provide local language translations of this EULA in some locations. You agree those translations are provided for informational purposes only and if there is any inconsistency, the English version of this EULA will prevail.

12.16 **Order of Precedence**. If there is any conflict between this EULA and any applicable Cisco policy expressly referenced in this EULA, the order of precedence is:

(a) this EULA (excluding any Cisco policies); then

(b) any applicable Cisco policy expressly referenced in this EULA and any agreement expressly incorporated by reference.

13. Definitions

"**Affiliate**" means any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where "control" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (e.g., a contract that allows control).

"**Approved Source**" means Cisco or a Cisco Partner.

"**Authorized Third Parties**" means Your Users, Your Affiliates, Your third party service providers, and each of their respective Users, permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement.

"**Cisco**" "**we**" "**our**" or "**us**" means Cisco Systems, Inc. or its applicable Affiliate(s).

"**Cisco Content**" means any:

(a) content or data provided by Cisco to You as part of Your use of the Cisco Technology; and

(b) content or data that the Cisco Technology generates or derives in connection with Your use.

Cisco Content includes geographic and domain information, rules, signatures, threat intelligence and data feeds and Cisco's compilation of suspicious URLs.

"**Cisco Partner**" means a Cisco authorized reseller, distributor or systems integrator authorized by Cisco to sell Cisco Technology.

"**Cloud Service**" means the Cisco hosted software-as-a-service offering or other Cisco cloud-enabled feature described in the applicable Product Specific Terms. Cloud Service includes applicable Documentation and may also include Software.

"**Confidential Information**" means non-public proprietary information of the disclosing party ("**Discloser**") obtained by the receiving party ("**Recipient**") in connection with this EULA, which:

(a) is conspicuously marked as confidential or if verbally disclosed, is summarized in writing to the Recipient within 14 days and marked as confidential; or

(b) is information which by its nature should reasonably be considered confidential whether disclosed in writing or verbally.

"**Delivery Date**" means the date agreed in Your Entitlement, or if no date is agreed:

(a) where Usage Rights in Software or Cloud Services are granted separately:

  (1) for Software, the earlier of the date Software is made available for download or installation, or the date that Cisco ships the tangible media containing the Software; and

  (2) for Cloud Services, the date on which the Cloud Service is made available for Your use; or

(b) where Usage Rights in Software and Cloud Services are granted together, the earlier of the date Software is made available for download, or the date on which the Cloud Service is made available for Your use.

"**Documentation**" means the technical specifications and usage materials officially published by Cisco specifying the functionalities and capabilities of the applicable Cisco Technology.

"**Entitlement**" means the specific metrics, duration, and quantity of Cisco Technology You commit to acquire from an Approved Source through individual acquisitions or Your participation in a Cisco buying program.

"**Malicious Code**" means code designed or intended to disable or impede the normal operation of, or provide unauthorized access to, networks, systems, Software or Cloud Services other than as intended by the Cisco Technology (for example, as part of some of Cisco's security products).

"**Software**" means the Cisco computer programs, including Upgrades, firmware and applicable Documentation.

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

"**Usage Term**" means the period commencing on the Delivery Date and continuing until expiration or termination of the Entitlement, during which period You have the right to use the applicable Cisco Technology.

"**User**" means the individuals (including contractors or employees) permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement.

"**You**" means the individual or legal entity acquiring Usage Rights in the Cisco Technology.

[signature page follows]

The signatures below apply only to the foregoing Cisco End User License Agreement.

State of Michigan	**Cisco Systems, Inc.**
Authorized Signature	Authorized Signature
Print Name	Print Name
Title	Title
Month/Day/Year Date	Month/Day/Year Date