State of New Hampshire

DEPARTMENT OF ADMINISTRATIVE SERVICES
25 Capitol Street – Room 100
Concord, New Hampshire 03301
(603) 271-3201 Office@das.nh.gov

Charles M. Arlinghaus
Commissioner

Catherine A. Keane
Deputy Commissioner

Sheri L. Rockburn
Assistant Commissioner

August 7, 2024

His Excellency, Governor Christopher T. Sununu
   and the Honorable Council
State House
Concord, New Hampshire 03301

REQUESTED ACTION

Authorize the Department of Administrative Services to enter into a contract with Facilities Management Express, LLC, (VC #488333), Columbus, OH in an amount up to and not to exceed $298,452.00 for maintenance software, with the option to renew for up to an additional two-year period, effective upon Governor and Council approval for the period September 1, 2024, through August 31, 2029.

Funding shall be provided through individual agency expenditures, none of which shall be permitted unless there are sufficient appropriated funds to cover the expenditure.

EXPLANATION

The Department of Administrative Services (DAS), through the Bureau of Purchase and Property (BoPP), issued request for proposal (RFP) 2859-24 on January 22, 2024, with responses due on March 1, 2024. This bid reached 152 vendors through the NIGP registry with an additional 21 directly sourced. There were 7 responses received with Facilities Management Express, LLC submitting the highest total score.

The tables below summarize the comprehensive scoring completed by the Department of Information Technology (DoIT); Central Facilities Bureau (CFB), DAS; Bureau of Courts (BoC), DAS; and BoPP, DAS. The scoring team was comprised of Rebecca Bolton, DoIT; Robert Kelley, DoIT; Donald Perrin, CFB; Brigitte Proctor, CFB; Ruth Kimball, BoC; and Jonah Rosa, BoPP Senior Purchasing Agent.

Facilities Management Express, LLC Awarded Points		
Category	Possible points	Points Awarded
Proposed Software Solution & Vendor Presentation	20	20
Vendor's Technical, Service, and Project Management Experience	15	15
Bidder Qualifications / Experience	15	15
Price proposal	50	43
Total	**100**	**93**

This contract (Contract #8003483), upon approval, will enable state agencies to streamline their maintenance work order process resulting in a significant decrease in the amount of time needed to manage the maintenance workflow and potential cost savings regarding energy efficiency, labor costs, and equipment upkeep costs by tracking key performance indicators with this new software. The existing software has very limited capabilities and cannot keep up with the demand. For example, the current software requires end users to manually enter a work order request which generates an email whereby the maintenance technician manually creates the workorder. Additionally, there is no ability to communicate the work order status within the system which requires all parties to call or email for updates in addition to manually entering the status in the current software as each stage of the maintenance process is accomplished. Although some migration is anticipated after contract implementation, it is expected to be minimal.

The requested price limitation of $298,452.00 will cover the full term of the contract including ongoing customer support and is based off the pricing provided in Facilities Management Express, LLC's proposal. The spend limitation will be closely monitored to prevent the contract price limitation from being exceeded.

Contract financials	
Year 1 cost (including implementation)	$79,200.000
Year 2 cost	$52,800.00
Year 3 cost	$52,800.00
Year 4 cost	$55,440.00
Year 5 cost	$58,212.00
Recommended price limitation	$298,452.00

Based on the foregoing, I am respectfully recommending approval of the contract with Facilities Management Express, LLC.

Respectfully submitted,

Charles M. Arlinghaus
Commissioner

\

Denis Goulet
Commissioner

June 26, 2024

Charles M. Arlinghaus, Commissioner
Department of Administrative Services
State of New Hampshire
25 Capitol Street – Room 100
Concord, NH 03301

Dear Commissioner Arlinghaus:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a contract with Facilities Management Express, LLC, as described below and referenced as DoIT No. 2024-071.

The purpose of this request is to provide maintenance software that will enable state agencies to streamline their maintenance work order process.

The Total Price Limitation shall be $298,452 effective upon Governor and Council approval for the period of September 1, 2024 through August 31, 2029.

A copy of this letter must accompany the Department of Administrative Services' submission to the Governor and Executive Council for approval.

Sincerely,

Denis Goulet

DG/jd
DoIT #2024-071

cc: Cindy Dotlich, IT Manager

Division of Procurement Support Services
Bureau of Purchase Property

RFP Scoring Summary

Gary S. Lunetta
Director
(603) 271-2201

Bid Description	Computerized Maintenance Management Software		
RFP#	2859-24	Agency	Statewide
Agent Name	Jonah Rosa	Bid Closing	2/21/2024 @ 9:30 AM

Indicates highest overall score: ■

Vendor	Financial Score	Technical Score	Total Score
Agelix consulting	50	14	64
Asset Works	15	40	55
Atom	19	32	51
Brightly	29	46	75
FMX	43	50	93
IBM	7	18	25
RTA	17	17	34

*Final scoring is consensus based

Financial Scoring

Indicates Lowest Cost: ■

	Agelix Consulting				Asset Works				
	License Costs	Barcode Scanning Gun	Barcode Printer	fees for every 1,000 work orders over the 15,000 work order (WO) base limit per year	License Costs	Barcode Scanning Gun	Barcode Printer	Implementation	License Costs
Year 1	$46,500.00			$3,000.00	$120,000.00			$214,040.00	$70,000.00
Year 2	$47,430.00			$3,075.00	$126,000.00			N/A	$70,000.00
Year 3	$48,379.00			$3,150.00	$132,300.00			N/A	$70,000.00
Year 4	$49,347.00			$3,225.00	$138,915.00			N/A	$70,000.00
Year 5	$50,334.00			$3,300.00	$145,910.75			N/A	$70,000.00
Subtotal	$241,990.00	$0.00	$0.00	$15,750.00	$663,125.75	$0.00	$0.00	$214,040.00	$350,000.00
Total Cost	$257,740.00				$877,165.75				
Total Points	50				15				
	FMX				IBM				
	License Costs	Barcode Scanning Gun	Barcode Printer	Implementation	License Costs (Maximo Application Suite per AppPoint Subscription License)	License Costs (Maximo Application Suite per AppPoint Subscription License SaaS)	Barcode Printer	Implementation	License Costs
Year 1	$52,800.00	can use smartphone or tablet	$26,400.00	$707,513.00	$162,453.60			$140,000.00	

Division of Procurement Support Services
Bureau of Purchase Property

RFP Scoring Summary

Gary S. Lunetta
Director
(603) 271-2201

Year 2	$52,800.00			N/A		$170,576.28			Based on Tiers
Year 3	$52,800.00			N/A		$179,105.09			and Number of
Year 4	$55,440.00			N/A		$188,060.35			Assets
Year 5	$58,212.00			N/A		$197,463.37			
Subtotal	$272,052.00	$0.00	$0.00	$26,400.00	$707,513.00	$897,658.69	$0.00	$140,000.00	$0.00
Total Cost	$298,452.00					$1,745,171.69			
Total Points	43					7			

Technical Scoring				
Indicates Highest Score: ▪	Proposed Software Solution & Vendor Presentation	Vendor's Technical, Service, and Project Management Experience	Bidder Qualifications / Experience	Total Points
	20 possible points	15 possible points	15 possible points	50 possible points
Agelix	6	4	4	14
Asset Works	15	12	13	40
Atom	12	12	8	32
Brightly	18	14	14	46
▪▪▪	20	15	15	50
IBM	8	5	5	18
RTA	7	5	5	17

Recommendation Summary	
Statewide Contract or Amendment	Statewide Contract
Term of Contract	5 years with the option to extend for 2 years
Price Limitation	$298,452.00
Number of Solicitations Received	7
Number of Sourced Bidders	21
Number of NIGP Vendors Sourced	152
Number of non-responsive bidders	166
P-37 Checklist Complete	Yes
D&B Report Attached	No
Method of Payment (P-card/ACH)	P-card and ACH
FOB Delivered	Yes
Expiring Contract Price Limitation	N/A
Total Cost Savings ($/%)	$140,804.52 47% when compared to the next low bid

Division of Procurement Support Services
Bureau of Purchase Property

RFP Scoring Summary

Gary S. Lunetta
Director
(603) 271-2201

Scoring Team		
Name	**Title**	**Department**
Jonah Rosa	Senior Purchasing Agent	Bureau of Purchase and Property
Donald Perrin	Superintendant of Plant & Property	Central Facilities Bureau
Brigitte Proctor	Facilities Data Assistant	Central Facilities Bureau
Rebecca Bolton	IT Lead	Department of Internet Technology
Robert Kelley	IT Lead	Department of Internet Technology
Ruth Kimball	Project Manager	Bureau of Courts

Special Notes:

Division of Procurement Support Services
Bureau of Purchase Property

RFP Scoring Summary

Gary S. Lunetta
Director
(603) 271-2201

Atom			Brightly			
Barcode Scanning Gun (unit price)	Barcode Printer (unit price)	Implementation	License Costs	Barcode Scanning Gun	Barcode Printer	Implementation
$500.00	$400.00	$325,000.00	$62,459.51	not proposed	not proposed	$27,902.14
			$79,754.40			N/A
			$84,539.66			N/A
			$89,612.04			N/A
			$94,988.77			N/A
$500.00	$400.00	$325,000.00	$411,354.38	$0.00	$0.00	$27,902.14
$675,900.00			$439,256.52			
19			29			

RTA			RTA Pricing:
Barcode Scanning Gun	Barcode Printer	Other Costs	

Concierge

Asset Block	Annual MSRP	Per Asset Annual	Per Asset Per Month
100	-	-	-
500	$71,008	$142.00	$11.83
1,000	$103,207	$103.00	$8.60

Diamond

Asset Block	Annual MSRP	Per Asset Annual	Per Asset Per Month
100	-	-	-
500	$47,339	$94.68	$7.89
1,000	$68,805	$68.81	$5.73

Division of Procurement Support Services
Bureau of Purchase Property

RFP Scoring Summary

Gary S. Lunetta
Director
(603) 271-2201

$0.00	$0.00	$0.00

$750,422.00
17

5,000	$409,615	$82.00	$6.83
10,000	$650,285	$65.00	$5.42
20,000	$1,032,360	$52.00	$4.30
50,000	$2,048,653	$41.00	$3.41

Fleet Valet level Implementation & Hardware Included

5,000	$273,077	$54.62	$4.55
10,000	$433,523	$43.35	$3.61
20,000	$688,240	$34.41	$2.87
50,000	$1,365,769	$27.32	$2.28

Fleet Valet level Implementation & Hardware Included

Platinum

Asset Block	Annual MSRP	Per Asset Annual	Per Asset Per Month
100	$9,600	$96.00	$8.00
500	$32,340	$64.68	$5.39
1,000	$49,804	$49.80	$4.15
5,000	$191,744	$38.35	$3.20
10,000	$295,286	$29.53	$2.46
20,000	$454,740	$22.74	$1.89
50,000	$875,374	$17.51	$1.46

Implementation & Hardware Sold Separately

Gold

Asset Block	Annual MSRP	Per Asset Annual	Per Asset Per Month
100	$7,200	$72.00	$6.00
500	$23,813	$48.00	$3.97
1,000	$37,805	$38.00	$3.15
5,000	$150,042	$30.00	$2.50
10,000	$238,200	$24.00	$1.98
20,000	$378,154	$19.00	$1.58
50,000	$750,422	$15.00	$1.25

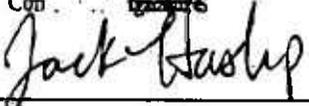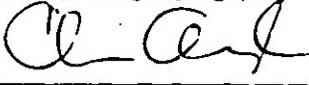**Implementation & Hardware Sold Separately**

Notice: This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

AGREEMENT
The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS

1. IDENTIFICATION.

1.1 State Agency Name Department of Administrative Services Bureau of Purchase and Property	1.2 State Agency Address 25 Capitol Street, Room 102 Concord, NH 03301
1.3 Contractor Name Facilities Management Express, LLC	1.4 Contractor Address 800 Yard Street, Suite 115 Columbus, OH 43212

1.5 Contractor Phone Number (585) 705-7885	1.6 Account Unit and Class Various	1.7 Completion Date 8/31/2029	1.8 Price Limitation $298,452.00

1.9 Contracting Officer for State Agency Gary Lunetta, Director	1.10 State Agency Telephone Number (603) 271-3606
1.11 Con . . bnacurG *[signature]* Jack Haslip Date: 7/1/24	1.12 Name and Title of Contractor Signatory Jack Haslup VP-Finance
1.13 State Agency Signature *[signature]* Date: 7/15/24	1.14 Name and Title of State Agency Signatory Charles M. Arlinghaus, Commissioner

1.15 Approval by the N.H. Department of Administration, Division of Personnel *(if applicable)* By: Director, On:
1.16 Approval by the Attorney General (Form, Substance and Execution) *(if applicable)* By: *Duncan A. Edgar*   On: July 23, 2024
1.17 Approval by the Governor and Executive Council *(if applicable)* G&C Item number: G&C Meeting Date:

Contractor Initials JHH
Date 7/1/24

2. SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages contractor identified in block 1.3 ("Contractor") to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT B which is incorporated herein by reference ("Services").

3. EFFECTIVE DATE/COMPLETION OF SERVICES.
3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.13 ("Effective Date").
3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed.
3.3 Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT.
Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds. In no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds by any state or federal legislative or executive action that reduces, eliminates or otherwise modifies the appropriation or availability of funding for this Agreement and the Scope for Services provided in EXHIBIT B, in whole or in part, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to reduce or terminate the Services under this Agreement immediately upon giving the Contractor notice of such reduction or termination. The State shall not be required to transfer funds from any other account or source to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/ PAYMENT.
5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT C which is incorporated herein by reference.
5.2 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8. The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof and shall be the only and the complete compensation to the Contractor for the Services.
5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.
5.4 The State's liability under this Agreement shall be limited to monetary damages not to exceed the total fees paid. The Contractor agrees that it has an adequate remedy at law for any breach of this Agreement by the State and hereby waives any right to specific performance or other equitable remedies against the State.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/EQUAL EMPLOYMENT OPPORTUNITY.
6.1 In connection with the performance of the Services, the Contractor shall comply with all applicable statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal employment opportunity laws and the Governor's order on Respect and Civility in the Workplace, Executive order 2020-01. In addition, if this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all federal executive orders, rules, regulations and statutes, and with any rules, regulations and guidelines as the State or the United States issue to implement these regulations. The Contractor shall also comply with all applicable intellectual property laws.
6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of age, sex, sexual orientation, race, color, marital status, physical or mental disability, religious creed, national origin, gender identity, or gender expression, and will take affirmative action to prevent such discrimination, unless exempt by state or federal law. The Contractor shall ensure any subcontractors comply with these nondiscrimination requirements.
6.3 No payments or transfers of value by Contractor or its representatives in connection with this Agreement have or shall be made which have the purpose or effect of public or commercial bribery, or acceptance of or acquiescence in extortion, kickbacks, or other unlawful or improper means of obtaining business.
6.4 The Contractor agrees to permit the State or United States access to any of the Contractor's books, records and accounts for the purpose of ascertaining compliance with this Agreement and all rules, regulations and orders pertaining to the covenants, terms and conditions of this Agreement.

7. PERSONNEL.
7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services and shall be properly licensed and otherwise authorized to do so under all applicable laws.
7.2 The Contracting Officer specified in block 1.9, or any successor, shall be the State's point of contact pertaining to this Agreement.

Contractor Initials JH

Date 7/1/24

8. EVENT OF DEFAULT/REMEDIES.

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

8.1.1 failure to perform the Services satisfactorily or on schedule;

8.1.2 failure to submit any report required hereunder; and/or

8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) calendar days from the date of the notice; and if the Event of Default is not timely cured, terminate this Agreement, effective two (2) calendar days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 give the Contractor a written notice specifying the Event of Default and set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 give the Contractor a written notice specifying the Event of Default, treat the Agreement as breached, terminate the Agreement and pursue any of its remedies at law or in equity, or both.

9. TERMINATION.

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, terminate the Agreement for any reason, in whole or in part, by thirty (30) calendar days written notice to the Contractor that the State is exercising its option to terminate the Agreement.

9.2 In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall, at the State's discretion, deliver to the Contracting Officer, not later than fifteen (15) calendar days after the date of termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. In addition, at the State's discretion, the Contractor shall, within fifteen (15) calendar days of notice of early termination, develop and submit to the State a transition plan for Services under the Agreement.

10. PROPERTY OWNERSHIP/DISCLOSURE.

10.1 As used in this Agreement, the word "Property" shall mean all data, information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

10.2 All data and any Property which has been received from the State, or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

10.3 Disclosure of data, information and other records shall be governed by N.H. RSA chapter 91-A and/or other applicable law. Disclosure requires prior written approval of the State.

11. CONTRACTOR'S RELATION TO THE STATE.
In the performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS.

12.1 Contractor shall provide the State written notice at least fifteen (15) calendar days before any proposed assignment, delegation, or other transfer of any interest in this Agreement. No such assignment, delegation, or other transfer shall be effective without the written consent of the State.

12.2 For purposes of paragraph 12, a Change of Control shall constitute assignment. "Change of Control" means (a) merger, consolidation, or a transaction or series of related transactions in which a third party, together with its affiliates, becomes the direct or indirect owner of fifty percent (50%) or more of the voting shares or similar equity interests, or combined voting power of the Contractor, or (b) the sale of all or substantially all of the assets of the Contractor.

12.3 None of the Services shall be subcontracted by the Contractor without prior written notice and consent of the State.

12.4 The State is entitled to copies of all subcontracts and assignment agreements and shall not be bound by any provisions contained in a subcontract or an assignment agreement to which it is not a party.

13. INDEMNIFICATION.
The Contractor shall indemnify, defend, and hold harmless the State, its officers, and employees from and against all actions, claims, damages, demands, judgments, fines, liabilities, losses, and other expenses, including, without limitation, reasonable attorneys' fees, arising out of or relating to this Agreement directly or indirectly arising from death, personal injury, property damage, intellectual property infringement, or other claims asserted against the State, its officers, or employees caused by the acts or omissions of negligence, reckless or willful misconduct, or fraud by the Contractor, its employees, agents, or subcontractors. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph 13. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the State's sovereign immunity, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

Contractor Initials _JHH_

Date _7/1/24_

14.1 The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:

14.1.1 commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than $1,000,000 per occurrence and $2,000,000 aggregate or excess; and

14.1.2 special cause of loss coverage form covering all Property subject to subparagraph 10.2 herein, in an amount not less than 80% of the whole replacement value of the Property.

14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.

14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or any successor, a certificate(s) of insurance for all insurance required under this Agreement. At the request of the Contracting Officer, or any successor, the Contractor shall provide certificate(s) of insurance for all renewal(s) of insurance required under this Agreement. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference.

15. WORKERS' COMPENSATION.

15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A *("Workers' Compensation")*.

15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. The Contractor shall furnish the Contracting Officer identified in block 1.9, or any successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. WAIVER OF BREACH. A State's failure to enforce its rights with respect to any single or continuing breach of this Agreement shall not act as a waiver of the right of the State to later enforce any such rights or to enforce any other or any subsequent breach.

17. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

18. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire unless no such approval is required under the circumstances pursuant to State law, rule or policy.

19. CHOICE OF LAW AND FORUM.

19.1 This Agreement shall be governed, interpreted and construed in accordance with the laws of the State of New Hampshire except where the Federal supremacy clause requires otherwise. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party.

19.2 Any actions arising out of this Agreement, including the breach or alleged breach thereof, may not be submitted to binding arbitration, but must, instead, be brought and maintained in the Merrimack County Superior Court of New Hampshire which shall have exclusive jurisdiction thereof.

20. CONFLICTING TERMS. In the event of a conflict between the terms of this P-37 form (as modified in EXHIBIT A) and any other portion of this Agreement including any attachments thereto, the terms of the P-37 (as modified in EXHIBIT A) shall control.

21. THIRD PARTIES. This Agreement is being entered into for the sole benefit of the parties hereto, and nothing herein, express or implied, is intended to or will confer any legal or equitable right, benefit, or remedy of any nature upon any other person.

22. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

23. SPECIAL PROVISIONS. Additional or modifying provisions set forth in the attached EXHIBIT A are incorporated herein by reference.

24. FURTHER ASSURANCES. The Contractor, along with its agents and affiliates, shall, at its own cost and expense, execute any additional documents and take such further actions as may be reasonably required to carry out the provisions of this Agreement and give effect to the transactions contemplated hereby.

25. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

26. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

Contractor Initials: GH

Date 7/11/24

EXHIBIT A - SPECIAL PROVISIONS

There are no special provisions of this contract.

Contractor Initials J4H

Date 7/1/24

EXHIBIT B - SCOPE OF SERVICES

1. **INTRODUCTION:**
   1.1. Facilities Management Express, LLC (hereinafter referred to as the "Contractor") hereby agrees to provide the State of New Hampshire (hereinafter referred to as the "State"), Department of Administrative Services, with Computerized Maintenance Management Software in accordance with the proposal submission in response to State Request for Proposal 2859-24 and as described herein.

2. **CONTRACT DOCUMENTS:**
   2.1. This Contract consists of the following documents ("Contract Documents"):
      2.1.1. State of New Hampshire Terms and Conditions, General Provisions Form P-37
      2.1.2. EXHIBIT A   Special Provisions
      2.1.3. EXHIBIT B   Scope of Services
      2.1.4. EXHIBIT C   Method of Payment
      2.1.5. EXHIBIT D   RFP 2859-24
      2.1.6. EXHIBIT E   Contractor's Proposal Response
   2.2. In the event of any conflict among the terms or provisions of the documents listed above, the following order of priority shall indicate which documents control: (1), Form Number P-37 as modified by EXHIBIT A "Special Provisions, (2) EXHIBIT B "Scope of Services," (3) EXHIBIT C "Method of Payment," (4) EXHIBIT D "RFP 2859-24," and (5) EXHIBIT E "Contractor's Proposal Response."

3. **TERM OF CONTRACT:**
   3.1. The term of the contract shall commence on upon approval of the Governor and Executive Council through August 31, 2029, a period of approximately five (5) years.

   3.2. The Contract may be extended for up to an additional two (2) years thereafter upon the same terms, conditions, and pricing structure with the approval of the Governor and Executive Council.

   3.3. The maximum term of the Contract (including all extensions) cannot exceed seven (7) years.

4. **SCOPE OF WORK:**
   4.1. The Contractor shall provide the State of New Hampshire with access to Computerized Maintenance Management Software with the following functionality at a minimum, but not limited to:
      4.1.1. Support additional State Agencies in the future
      4.1.2. Demo / Training Videos or Guides
      4.1.3. Supporting approximately 50 administrators (individuals with approval authority) and up to 100 other users (individuals who submit work requests)
      4.1.4. Permit multiple approval levels (i.e., Requestor, Technician, Supervisor, Approver, etc.)
      4.1.5. Mass data import/export
      4.1.6. Barcode/QR code capable
      4.1.7. Preventative maintenance scheduling
      4.1.8. Automatic notifications at each stage of the work order process
      4.1.9. Permits communication between users
      4.1.10. Generate Work Orders
      4.1.11. Asset inventory
      4.1.12. KPI Reporting – asset usage, labor, materials, performance trends
      4.1.13. Track Vendors who may complete work orders
      4.1.14. Cloud based/Web Access
      4.1.15. Mobile App and Mobile Webpage for access from Android and/or Apple products
      4.1.16. Ongoing Customer Support

Contractor Initials JGH

Date 7/1/24

4.2. Implementation:

Test phase	Contractor Role/ Responsibility	State Role/ Responsibility	Tools	Timeframe
Management of the testing process	Y	N	SDLC tracking system	Ongoing
Test planning	Y	Acceptance testing only	SDLC tracking system	Ongoing
Test scenario development	Y	Acceptance testing only	SDLC tracking system	Ongoing
Data preparation	Y	Acceptance testing only	SDLC tracking system	Ongoing
System preparation	Y	N	Test environments	Ongoing
Unit testing	Y	N	Source code	Ongoing
System integration testing	Y	N	Source code	Ongoing
User acceptance testing	N	Y	Customer site	Optional upon implementation
System performance testing	Y	N	Test environments	Ongoing
Defect tracking	Y	N	SDLC tracking system	Ongoing

Meetings and Processes Through Launch	Estimated Days (Recommended)
Kickoff Meeting	Day 0
Data Review and Pre-Site Configuration • Data Input • Pre-Site Configuration • Single Sign-On (SSO)	Days 1-7
Admin Training • Data review • Workflow review • Admin settings review	Days 8-14
Training • Staff Training • Launch	Days 15-21
Post-Launch • One Month Post Launch	Day 21

4.2.1. The Contractor shall provide:

4.2.1.1. **Customer Success Manager** responsible for project oversight and collaboration with client project management team, FMX site configuration, oversight of mass data importing, and client training.

4.2.1.2. **Customer Success Specialist** responsible for mass data importing, SSO login button configuration, existing integration configuration.

4.2.1.3. **Account Manager** responsible for the management of client projects post-launch and sharing FMX product innovations throughout the lifetime of this contract.

4.2.2. The State shall provide:

4.2.2.1. **State Contacts** responsible for project oversight, resource management, stakeholder interactions and liaison, existing process flows, setup, configuration, and customization of the FMX workflows.

Contractor Initials JHH

Date 7/1/24

4.2.2.2. **State Process Owners/Stakeholders** responsible for participating in requirements gathering, prioritizing requirements.

4.2.2.3. **State Administrators** responsible for participating in existing process plows, setup, configuration, and customization of the FMX workflows, daily administration of FMX post-launch.

4.2.2.4. **Data for Importing** within seven (7) days prior to the kickoff meeting. This data shall contain user, equipment, and building information in Microsoft Excel, CSV, SQL, or JSON formats. PDF, scans, or paper copies are not acceptable.

4.3. **Training:** The Contractor shall provide training on the use of their software as needed with no additional costs to the State. In-depth training on all necessary workflow items for each training group Training formats available: Webinar, self-service via pre-recorded video, self- service via written training guides

4.4. **Software Updates:** The contractor shall automatically provide system security updates as they become available at no cost to the State during off-peak hours. Functional changes to the portal as requested by the State shall be provided at no cost and no more than 60 days from the date of notification to the Contractor. All updates shall be deployed by the Contractor remotely. The Contractor shall notify all end users within 30 days of any updates that require the software to be off-line for an extended period.

4.5. **Data Security:**

4.5.1. The Contractor's hosting provider, Microsoft Azure shall follow NIST SP 800 controls at a minimum.

4.5.2. The software shall use intrusion detection systems, physical access mechanisms, and technical testing to protect against unauthorized access and modification.

4.5.3. The Contractor shall protect confidential data through encryption, access controls, and device security measures to ensure privacy. The Contractor shall also scan and update third- party libraries for security vulnerabilities.

4.5.4. Customers are notified by email as soon as possible when a confirmed data breach is discovered. In addition, the assigned Customer Success Manager will call the customer's primary contact to personally inform them of the situation.

4.5.5. The Contractor shall store three copies of all customer data within a primary data center and three copies within a geographically disparate secondary data center. Additionally, the Contractor shall perform differential database backups every hour, full database backups every week, and archive database backups for a period of 90 days. Extra procedures include redundant storage, load-balanced servers, and synchronized clocks using reputable time sources to ensure data integrity.

4.5.6. In addition to annual pen testing and monthly vulnerability scanning, the Contractor shall use automated and manual testing, OWASP top 10 checks, and identical production environment to ensure security.

4.5.7. The Contractor shall use a combination of internal and external resources to conduct security testing. We use third parties for annual penetration testing but also complete regular internal security testing via vulnerability scanning, code review, manual and automated testing.

4.5.8. The Contractor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Contractor's hosting infrastructure and/or the application upon request.

4.5.9. Servers, Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA and have latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.

4.6. **Data Storage:** There shall be no limitations on data storage. The Contractor shall store data indefinitely barring the cancellation of this contract. In the event the State decides to cancel this contract, all data shall be exported to excel or csv and provided to the State at no additional cost.

Contractor Initials JGH

Date 7/11/24

4.7. **Customer Service:** The Contractor shall provide customer service to the State at no additional cost Monday through Friday, 8:00 am to 6:00 pm. All notification outside of these hours shall be sent via email. The Contractor shall assign a dedicated account representative and a backup in their absence who will be responsible for the daily administration of this Contract. The account representative shall be familiar with all Contract requirements to ensure compliance with the terms of the Contract. The account representative's responsibilities shall include but not be limited to:

4.7.1. Coordinate business review meeting(s) either virtually or on-site with the State held at a cadence requested by the State.

4.7.2. Provide recommended process and productivity improvements related to potential cost savings to the State for consideration quarterly.

4.7.3. Provide information and product offerings to bring the latest industry ideas and trends to the State as applicable.

4.7.4. Provide training on the use of the Contractor's portal as needed with no charge to the State.

4.8. **Support Classifications and Resolution:** Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer. The Contractor shall resolve critical defects within minutes or hours; high priority defects resolved either same day or 1-2 business days; medium priority defects resolved between 1-5 business days; low priority defects resolved between 1-14 business days.

4.9. **Performance Guarantee:** The Contractor shall ensure a 99% up-time rate measured annually. If the Contractor fails to meet the 99% up-time rate, then the Contractor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing within 30 days at the end of each 12-month period.

4.10. **Record of Activities:** The Contractor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.

4.11. **Disaster Recovery:**

4.11.1. Contractor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.

4.11.2. Contractor shall adhere to a defined and documented back-up schedule and procedure.

4.11.3. Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.

4.11.4. Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.

4.11.5. Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.

4.12. The Contractor shall support single sign-on (SSO) protocols via WS-Federation, Google OAuth, and SAML-P.

4.13. The Contractor shall permit use of the software on browsers such as Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, and Microsoft Internet Explorer.

4.14. Except as otherwise provided in this Scope of Services, all services performed under this Contract shall be performed Monday through Friday between the hours of 8:00 A.M. and 6:00 P.M. unless other arrangements are made in advance with the State. Any deviation in work hours shall be pre-approved by the Contracting

Contractor Initials

Date

Officer. The State requires ten-day advance knowledge of said work schedules to provide security and access to respective work areas.

4.15. The Contractor shall not commence work until a conference is held with each State agency intending to utilize the Contractor's services, at which representatives of the Contractor and the State are present. The conference will be arranged by the State agency.

4.16. The State shall require correction of any defective work and the repair of any damages to any part of a building, or its appurtenances caused by the Contractor or its employees, subcontractors, equipment or supplies. The Contractor shall correct, repair, or replace all defective work, as needed, to complete said work in satisfactory condition, and damages so caused in order to restore the building and its appurtenances to their previous condition. Upon failure of the Contractor to proceed promptly with the necessary corrections or repairs, the State may withhold any amount necessary to correct all defective work or repair all damages from payments to the Contractor.

4.17. The work staff shall consist of qualified persons completely familiar with the products and equipment that they will use. The Contracting Officer may require the Contractor to dismiss from the work such employees as the Contracting Officer deems incompetent, careless, insubordinate, or otherwise objectionable, or whose continued employment on the work is deemed to be contrary to the public interest or inconsistent with the best interest of security and the State.

4.18. Neither the Contractor nor its employees or subcontractors shall represent themselves as employees or agents of the State.

4.19. While on State property the Contractor, its employees, and its sub-contractors shall be subject to the authority and control of the State, but under no circumstances shall such persons be deemed to be employees of the State.

4.20. All personnel shall observe all regulations or special restrictions in effect at any State agency location at which services are to be provided.

4.21. The Contractor's personnel shall be allowed only in areas where services are to be provided. The use of State telephones by the Contractor, its employees, or its sub-contractors is prohibited.

4.22. If sub-contractors are to be utilized, Contractor shall provide information regarding the proposed sub-contractors including the name of the company, their address, contact person and three references for clients they are currently servicing. Approval by the State must be received prior to a sub-contractor starting any work.

5. ESTABLISHMENT OF ACCOUNTS:
5.1. Each State of New Hampshire agency shall have its own individual customer account number. There may also be instances where divisions or bureaus within an agency will need their own individual customer account numbers. Should any State of New Hampshire agency place an order under the contract, the Contractor agrees to establish an account within three business days from the date the order is placed. However, there shall be no delay in any shipment; the agency shall receive the items ordered in accordance with the delivery time required under this bid invitation, as if an account already exists for the agency.

6. USAGE REPORTING:
6.1. The Contractor shall submit a quarterly and annual usage report for analysis for each state agency or eligible participant. Reports are due no later than 30 days after the end of each calendar quarter to the Bureau of Purchase and Property, Jonah Rosa and sent electronic to Jonah.L.Rosa@DAS.NH.Gov. At a minimum, the Report shall include:

6.1.1. Contract Number

6.1.2. Utilizing Agency and Eligible Participant

6.1.3. Services/Products Purchased (showing the manufacturer, item, part number, and the final cost.)

6.1.4. Total Cost of all Services/Products Purchased. Ability to sort by agency/eligible participant.

6.1.5. In Excel format

Contractor Initials JGH

Date 7/1/12

7. OBLIGATIONS AND LIABILITY OF THE CONTRACTOR:

7.1. The Contractor shall provide Computerized Maintenance Management Software strictly pursuant to, and in conformity with, the specifications described in State RFB #2859-24, as described herein, and under the terms of this Contract.

7.2. It is the responsibility of the Contractor to maintain this contract and New Hampshire Vendor Registration with up to date contact information.

7.3. Contract specific contact information (Sales contact, Contractor contract manager, etc.) shall be sent to the State's Contracting Office listed in Box 1.9 of Form P-37.

7.4. Additionally, all updates i.e., telephone numbers, contact names, email addresses, W9, tax identification numbers are required to be current through a formal electronic submission to the Bureau of Purchase and Property at: https://das.nh.gov/purchasing/vendorregistration/(S(q0fzcv55qhaeqs45jpyq5i45))/welcome.aspx.

7.5. The Contractor shall agree to hold the State of NH harmless from liability arising out of injuries or damage caused while performing this work. The Contractor shall agree that any damage to building(s), materials, equipment, or other property during the performance of the service shall be repaired at its own expense, to the State's satisfaction.

8. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION LOWER TIER COVERED TRANSACTIONS:

8.1. The Contractor certifies, by signature of this contract, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal Department or Agency.

9. CONFIDENTIALITY & CRIMINAL RECORD:

9.1. If requested by the using agency, the Contractor and its employees, and Sub-Contractors (if any), shall be required to sign and submit a Confidential Nature of Department Records Form and a Criminal Authorization Records Form. These forms shall be submitted to the individual using agency prior to the start of any work.

Contractor Initials _JGH_

Date _7|1|24_

EXHIBIT C - METHOD OF PAYMENT

10. **CONTRACT PRICE:**
    10.1. The Contractor hereby agrees to provide Computerized Maintenance Management Software in complete compliance with the terms and conditions specified in Exhibit B for an amount up to and not to exceed a price of $298,452.00; this figure shall not be considered a guaranteed or minimum figure; however, it shall be considered a maximum figure from the effective date through the expiration date as indicated in Form P-37 Block 1.7.

11. **PRICING STRUCTURE:**
    11.1. Pricing is based on 95 licensed users (70 technicians, 20 primary users, 5 administrators).

Year 1	Year 2	Year 3	Year 4	Year 5
$79,200	$52,800	$52,800	$55,440	$58,212

    11.2. A one-time fee of $26,400.00 shall be charged for implementation and training.

12. **CONTRACTORS'S BALANCE OF PRODUCT LINE ITEMS:**
    12.1. The items in the Offer Section include the items most commonly purchased by State of New Hampshire agencies and shall be used for award purposes. During the term of contract, the State may purchase other items that relate to the product/categories represented herein from the successful Contractor's Balance of Product Line. All items ordered shall include all shipping/charges as specified above in "Bid Prices".

13. **INVOICE:**
    13.1. Itemized invoices shall be submitted monthly to the individual agency after the completion of the job/services and shall include a brief description of the work done along with the location of work.

    13.2. Contractor shall be paid within 30 days after receipt of properly documented invoice and acceptance of the work to the State's satisfaction.

    13.3. The invoice shall be sent to the address of the using agency under agreement.

14. **PAYMENT:**
    14.1. Payments may be made via ACH or P-Card. Use the following link to enroll with the State Treasury for ACH payments: https://www.nh.gov/treasury.

Contractor Initials JGH

Date 7/1/24

EXHIBIT D - RFB 2859-24

RFB 2859-24 is incorporated here within.

Contractor Initials JGH

Date 7/1/24

EXHIBIT E - CONTRACTOR'S PROPOSAL

Contractor's proposal is incorporated here within.

Contractor Initials JHH

Date 7/1/24

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that FACILITIES MANAGEMENT EXPRESS, LLC is a Ohio Limited Liability Company registered to transact business in New Hampshire on February 07, 2024. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 953707

Certificate Number: 0006699305

IN TESTIMONY WHEREOF.

I hereto set my hand and cause to be affixed the Seal of the State of New Hampshire. this 5th day of June A.D. 2024.

David M. Scanlan
Secretary of State

ACTIONS TAKEN IN WRITING
BY THE MANAGERS
OF
FACILITIES MANAGEMENT EXPRESS, LLC
WITHOUT A MEETING

June 27, 2024

The undersigned, being all of the Managers (the "**Managers**") of Facilities Management Express, LLC, an Ohio limited liability company (the "**Company**"), do hereby take, authorize, and approve the actions set forth in the following resolutions, without a meeting, pursuant to Section 5.1(h)(vii) of the Fourth Amended and Restated Operating Agreement of the Company (the "**Operating Agreement**"). Capitalized terms used but not defined herein shall have the meanings as set forth in the Operating Agreement.

Background

WHEREAS, the Managers have deemed it in the best interest of the Company to authorize the company's VP - Finance to execute any documents or agreements necessary for the company to participate in various RFP and Proposal processes that potential customers of the company may require.

Approval of the Authorization

NOW THEREFORE BE IT HEREBY RESOLVED, that the Authorization shall be, and it hereby is, authorized and approved by the Managers on behalf of the Company.

Enabling Authority

RESOLVED, that, in addition to the specific authorizations hereunder conferred, the VP - Finance of the Company shall be, and hereby is, authorized in the name and on behalf of the Company to take all such other and further actions, including, but not limited to, the execution, acknowledgment, delivery and filing of all such other and further documents, instruments and agreements as the VP - Finance may deem necessary, convenient or desirable, in order to effect the actions contemplated by and the purposes of the foregoing resolutions, with the execution, delivery or filing of any such instrument or the taking of any such action as conclusive evidence of the authority of the VP - Finance to so act.

Ratification of Past Actions

RESOLVED, that any and all actions heretofore taken by or on behalf of the Managers, officers, employees or agents of the Company in connection with the

foregoing resolutions shall be, and the same hereby are, in all respects adopted, approved, ratified and confirmed on behalf of the Company.

Counterpart Signatures

RESOLVED, that these Actions may be executed in counterparts and by facsimile or other electronic transmission, all of which counterparts shall be deemed originals, all of which counterparts taken together shall constitute a single instrument, and the signature pages of each such counterpart may be detached from the several counterparts and attached to a single copy of this document to physically form a single instrument.

[Signatures on following page]

IN WITNESS WHEREOF, the undersigned have signed these Actions effective as of the date noted below.

MANAGERS:

Brian Gregory   6-27-24
Brian D. Gregory   Date

Todd L. Mace   6-27-24
Todd L. Mace   Date

Jeffrey M Wilkins   6-27-24
Jeffrey M. Wilkins   Date

_____   _____
Joe Onofrio   Date

IN WITNESS WHEREOF, the undersigned have signed these Actions effective as of the date noted below.

MANAGERS:

Brian Gregory
_____
Brian D. Gregory

6-27-24
_____
Date

_____
Todd L. Mace

_____
Date

Jeffrey M Wilkins
_____
Jeffrey M. Wilkins

6-27-24
_____
Date

Joseph Onofrio
_____
Joe Onofrio

6-27-24
_____
Date

[Signature Page for Actions Taken in Writing]

ACORD® CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
6/5/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER License # 1529	CONTACT NAME:		
The Keenan Agency 6805 Avery Mulrfield Drive Suite 200 Dublin, OH 43016	PHONE (A/C, No, Ext): (614) 764-7000		FAX (A/C, No): (614) 389-4259
	E-MAIL ADDRESS:		
	INSURER(S) AFFORDING COVERAGE		NAIC #
	INSURER A : VALLEY FORGE INSURANCE COMPANY		20508
INSURED	INSURER B : CONTINENTAL CAS CO		35289
FACILITIES MANAGEMENT EXPRESS LLC 800 YARD STREET, STE 115 GRANDVIEW HEIGHTS, OH 43212	INSURER C : BEAZLEY USA SERVCIES Inc.		37540
	INSURER D :		
	INSURER E :		
	INSURER F :		

COVERAGES   CERTIFICATE NUMBER: REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE [X] OCCUR			6025082990	1/10/2024	1/10/2025	EACH OCCURRENCE	$ 2,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 2,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER: POLICY [X] PRO-JECT LOC OTHER:						GENERAL AGGREGATE	$ 4,000,000
							PRODUCTS - COMP/OP AGG	$ 4,000,000
								$
A	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY / SCHEDULED AUTOS X HIRED AUTOS ONLY / X NON-OWNED AUTOS ONLY			6025082990	1/10/2024	1/10/2025	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
B	X UMBRELLA LIAB X OCCUR EXCESS LIAB CLAIMS-MADE DED X RETENTION $ 10,000			7034105103	1/10/2024	1/10/2025	EACH OCCURRENCE	$ 1,000,000
							AGGREGATE	$ 1,000,000
								$
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A		6025082990	1/10/2024	1/10/2025	PER STATUTE / X OTH-ER	
							E.L. EACH ACCIDENT	$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000
C	Professional Liab			W15C4721801	6/6/2024	6/6/2025	Per Claim	2,000,000
C	Cyber Liability			W15C4721801	6/6/2024	6/6/2025	Aggregate	2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER	CANCELLATION
State of New Hampshire Bureau of Purchasing and Property 25 Capitol Street Concord, NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)   © 1988-2015 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD
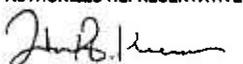
Response to RFP# 2859-24 Computerized Maintenance Management Software Implementation

STATE OF NEW HAMPSHIRE

Department of Administration
Division of Procurement and Support Services
Bureau of Purchase and Property

Delivered by

Facilities Management Express
Ameshia Williams, Account Executive
585-705-7885 | ameshia.williams@gofmx.com

Due Date: February 7, 2024 11:00 AM (EST) Computerized Maintenance Management Software Implementation

Facilities Management Express
800 Yard St #115
Grandview Heights, OH 43212

Cover letter

To Whom it May Concern,

Thank you for the opportunity to bid on your project at the State of New Hampshire. FMX provides purpose-built solutions for organizations that span facilities, maintenance, scheduling, and other operational-focused solutions. Having reviewed the contents of your Request for Proposal (RFP), I am confident that FMX can provide the solutions and services your organization needs to support your district and achieve your goals.

FMX serves over 1400 organizations nationwide. Hundreds of organizations have moved from other software tools to FMX over the past several years, with each noting that FMX understands the unique challenges that these organizations face while providing an easy-to-use, configurable solution that supports the key aspects of facility operations.

Enclosed is our response to your RFP, which we hope illustrates the solutions we offer and the value we provide. We look forward to working with the State of New Hampshire and serving you for years to come.

Best Regards,

Mike Manuche
mike.manuche@gofmx.com
VP of Sales, FMX

Table of contents (PDF Pages)

APPENDIX B - STATE OF NEW HAMPSHIRE TRANSMITTAL LETTER

Date: 2/19/2024

Company Name: FACILITIES MANAGEMENT Express, LLC
Address: 800 Yard Street, Suite 115
Columbus, OH 43212

To: Point of Contact: **Jonah Rosa**
Telephone: (603)-271-2550
Email: NH.Purchasing@das.nh.gov

RE: Proposal Invitation Name: **Computerized Maintenance Management System Implementation**
Proposal Number: **2859-24**
Proposal Posted Date (on or by): **1/22/2024**
Proposal Closing Date and Time: **2/7/2024 @ 11:00 AM (EST)**
Dear **Mr. Rosa,**

[Insert name of signor] John "Jack" Heslip , on behalf of Facilities Management Express, LLC [insert name of entity submitting proposal] (collectively referred to as "Vendor") hereby submits an offer as contained in the written proposal submitted herewith ("Proposal") to the State of New Hampshire in response to Proposal # 2859-24 for Computerized Maintenance Management System Implementation at the price(s) quoted herein in complete accordance with the proposal.

Vendor attests to the fact that:
1. The Vendor has reviewed and agreed to be bound by the Proposal.
2. The Vendor has not altered any of the language or other provisions contained in the Proposal document.
3. The Proposal is effective for a period of 180 days from the Proposal Closing date as indicated above.
4. The prices Vendor has quoted in the Proposal were established without collusion with other vendors.
5. The Vendor has read and fully understands this Proposal.
6. Further, in accordance with RSA 21-I:11-c, the undersigned Vendor certifies that neither the Vendor nor any of its subsidiaries, affiliates or principal officers (principal officers refers to individuals with management responsibility for the entity or association):
   a. Has, within the past 2 years, been convicted of, or pleaded guilty to, a violation of RSA 356:2, RSA 356:4, or any state or federal law or county or municipal ordinance prohibiting specified proposalding practices, or involving antitrust violations, which has not been annulled;
   b. Has been prohibited, either permanently or temporarily, from participating in any public works project pursuant to RSA 638:20;
   c. Has previously provided false, deceptive, or fraudulent information on a vendor code number application form, or any other document submitted to the state of New Hampshire, which information was not corrected as of the time of the filing a proposal, proposal, or quotation;
   d. Is currently debarred from performing work on any project of the federal government or the government of any state;
   e. Has, within the past 2 years, failed to cure a default on any contract with the federal government or the government of any state;
   f. Is presently subject to any order of the department of labor, the department of employment security, or any other state department, agency, board, or commission, finding that the applicant is not in compliance with the requirements of the laws or rules that the department, agency, board, or commission is charged with implementing;
   g. Is presently subject to any sanction or penalty finally issued by the department of labor, the department of employment security, or any other state department, agency, board, or commission, which sanction or penalty has not been fully discharged or fulfilled;
   h. Is currently serving a sentence or is subject to a continuing or unfulfilled penalty for any crime or violation noted in this section;
   i. Has failed or neglected to advise the division of any conviction, plea of guilty, or finding relative to any crime or violation noted in this section, or of any debarment, within 30 days of such conviction, plea, finding, or debarment; or
   j. Has been placed on the debarred parties list described in RSA 21-I:11-c within the past year.

This document shall be signed by a person who is authorized to legally obligate the responding vendor. A signature on this document indicates that all State of New Hampshire terms and conditions are accepted by the responding vendor and that any and all other terms and conditions submitted by the responding vendor are null and void, even if such terms and conditions have terminology to the contrary. The responding vendor shall also be subject to State of New Hampshire terms and conditions as stated on the reverse of the purchase order.

Authorized Signor's Signature: _John Jack Heslip_ Authorized Signor's Title: VP - Finance

18

Executive Summary

Core products

Maintenance Requests

Submit, prioritize and assign work requests across your organization to streamline communication and resolve issues faster. With Maintenance Requests, users will never have to worry about manually managing work order requests. FMX makes it quick and easy for requesters to submit work orders and stay up to date on progress. At the same time, staff can focus on resolving work orders with all the information they need right from their mobile device.
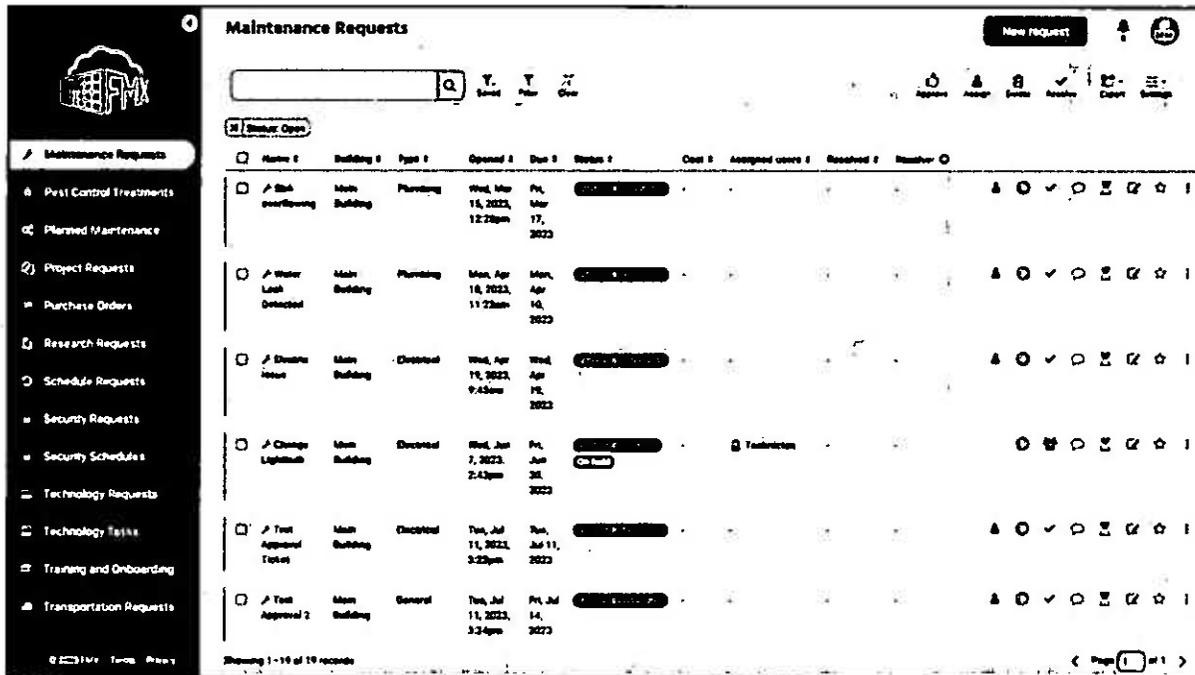
Key capabilities

- Use Calendar & To-Do views to easily to see schedules, upcoming tasks, and resolve conflicts by drag and drop rescheduling.

- Use your mobile device to quickly submit requests and ensure technicians can access all the

- Communicate in-app to directly update requestors, other technicians, vendors, and more.
- Save time with auto-assignment & notifications by assigning the technician best suited to the task and sending real-time updates.
- Configure custom request forms to ensure all relevant details are captured to complete the job - attach photos, videos, documents, and more.

- information they need to resolve work orders.
- Utilize QR code equipment tagging to submit requests, see work order history, or view equipment information.
- Gather actionable insights with interactive reporting & dashboards that track metrics like downtime, equipment repair cost, labor time and cost, and more.

Preventive Maintenance

Prevent costly equipment issues, and ensure your equipment is operating at peak performance. Use Preventive Maintenance to schedule regular inspections and upkeep tasks to prolong equipment life, reduce downtime, maintain safety, and avoid costly breakdowns.

Key capabilities

- Create and apply inspection checklists and instruction sets to tasks to ensure proper regulatory standards, equipment upkeep, and manufacturer-recommended service is completed.
- Schedule regular maintenance tasks using time-based and meter-based intervals. Store important records and other assets by uploading user manuals, warranties, and more.
- View the equipment log to see the previous work history for each equipment item.
- Use your mobile device to ensure technicians can access all the information they need to resolve work orders.
- Gather actionable insights with interactive reporting & dashboards that track metrics like downtime, equipment repair cost, labor time and cost, and more.

Equipment

Get the most value from your assets and equipment. Increase asset lifespans, reduce equipment downtime, and strategically plan capital investments with reliable maintenance software.

Key capabilities

- Centralize work order requests to make it easy for staff to submit, resolve, and see a history of work order requests.
- Schedule regular planned maintenance, like safety inspections, for equipment with time and meter-based intervals.
- Use QR codes to quickly see equipment details, previous work order history, or submit and resolve new work orders.
- Save time by auto-assigning the technician best suited to the task and sending real-time updates.

- View interactive reports and dashboards to see key metrics like costs, inventory usage, completion rates, and more.
- Create instruction sets and inspection checklists for all your inspections, cleanings, and QA testing.
- Integrate BAS, water/humidity/temperature sensor alerts, and more right into FMX to centralize facility operations.

Reporting & Dashboards

Capture, analyze, and discover actionable insights. With FMX, you can understand equipment repair trends, analyze labor cost and time, justify capital improvements, and plan your organization's budget expenditure.
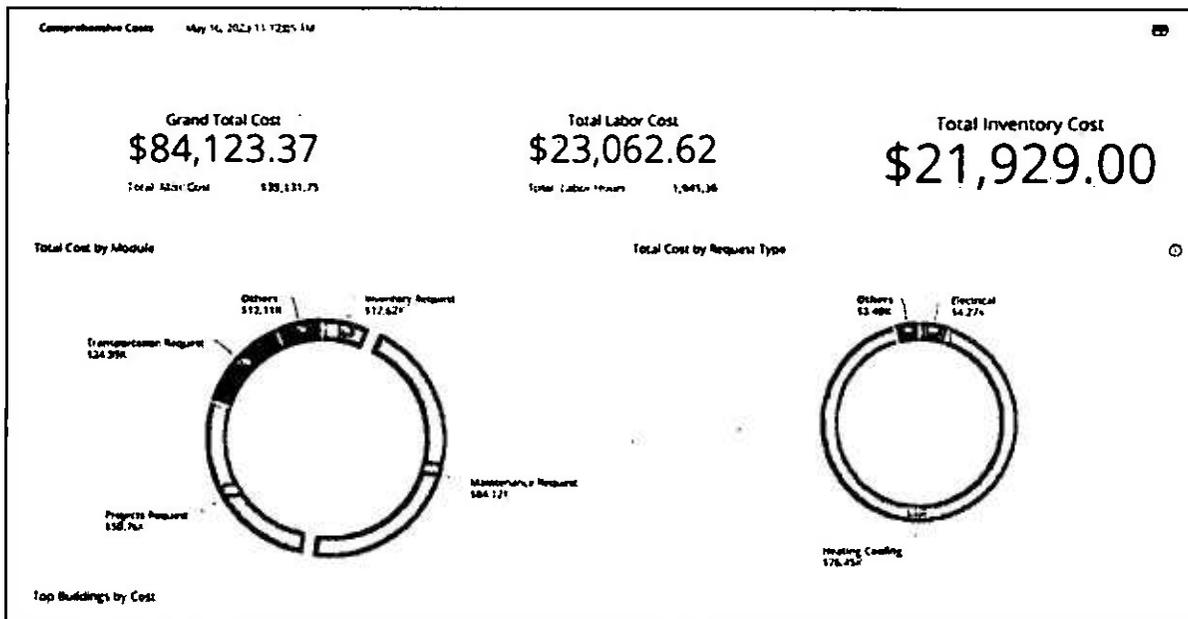
Key capabilities

- Interactive dashboards and filtering tools
- Insights on work orders, labor, equipment, inventory, invoicing, and capital forecasting
- Filterable by request type, building & location, date range, work state, user, and module

- Export for print and email distribution
- Standard dashboards for costs, operations, downtime, equipment, building usage, inventory usage, team performance, and work completed
- Custom-built reports can be purchased as an add-on

Professional services

The following services are **not*** included with the standard implementation:

Onsite Training

The FMX Customer Success Team will go to Customer's location for training on the FMX software.

SQL Update

Allows bulk actions to be performed by FMX Customer Success Team to a customer's FMX site. FMX will perform this service in the FMX offices and deploy this to the customer's account automatically. Customers may have to supply FMX with their desired changes to their FMX site. The time to complete this service varies widely from as little as 10 minutes to as long as 30 days.

Development Updates

Service is performed by the FMX Development team to perform a mass update to a customer's site. The service provided by the development team usually includes a change to the FMX software code. FMX will perform this service in the FMX offices and deploy this to the customer's account automatically. Customers may have to supply FMX with their desired changes to their FMX site. The time to complete this service varies widely depending on the customer requirement, which has spanned from 2 weeks to 30 days depending on many factors.

Data Management

The FMX Customer Success Team will perform the data management service and enter all data into a customer's FMX site not in the FMX acceptable data import formats. This service also includes a mass change in data to a customer's FMX site. FMX will perform this service in the FMX offices and deploy this to the customer's account automatically. Customers may have to supply FMX with their desired changes to their FMX site. The time to complete this service varies widely depending on the customer requirement, which has spanned from 2 weeks to 30 days depending on many factors.

*These services are available for an additional charge. To inquire about one of these services, reach out to your dedicated Customer Success Manager or Account Manager.

Watch our product tour

Want to see FMX in action? Watch our product demo, and experience an overview of our capabilities in full force.

www.gofmx.com/watchtour

Market differentiators

Customer success

Your needs warrant a streamlined implementation process that has you up and running and realizing ROI in a short time. The FMX customer success team is dedicated to providing it all to you, hiccup-free and with the resources that you need for fast staff adoption. The FMX Customer Success team that will support your implementation and our partnership:

- Boasts a market-best 98% CSAT (Customer Satisfaction) rating
- Has a 97% renewal rate, which is almost 4X better than the average SaaS company
- Has an average response time (calls, emails) of 60 minutes or less, compared to the industry average of 13 hours

Why FMX? Our approach

Our approach is simple, it all begins with listening and collaboration. FMX was created based on direct conversations with facilities and maintenance leaders, and that hasn't stopped. Input from professionals like you guides and informs our decisions, so FMX works the way you do. FMX's unique approach stands above the rest because of three key elements:

1. Ease of use
2. Configurability
3. Customer success

1. Ease of use

We believe in keeping things easy. Say goodbye to multiple emails, phone calls, and complicated paper forms. With a focus on ease of use and simplicity, your entire team will understand how to use FMX right out of the gate. Our software puts your day-to-day management on autopilot and frees up your time to make data-informed decisions and planning.

2. Configurability

With FMX, you're not stuck with a "standard model". FMX is designed to fuse with how you perform your operations—with an additional benefit of organizational structure and advanced record keeping. Hand-in-hand, our solutions are crafted with you.

3. Customer success

You're never alone, your needs warrant a streamlined implementation process that has you up and running and realizing ROI in a short time. The FMX customer service team is dedicated to providing it all to you, hiccup-free and with the resources that you need for fast staff adoption. Whether you're coming from paper or another system, we've seen it before. We've got your back with data migration assistance and continuous training for your staff and technicians.

Responses to Requirements and Deliverables

Work Order System Requirements	Additional Comments
Topic 1 - DESCRIPTION OF SOLUTION	
Question 1: Provide a detailed description of your proposed Solution, including features and functionality.	Please see pages 7-12 in the RFP response under Executive Summary.
Question 2: Describe how your Solution meets the business requirements in B-2 Business Requirements/Technical Requirements.	QUESTION REMOVED: NA.
Question 3: Describe ease of use and user friendliness of your proposed Solution including learning curve, navigation. Highlight in detail specific advantages to the user Interface. What methodology do you use to ensure that your user Interface is userfriendly?	FMX's unique approach stands above the rest because of three key elements: Ease of use, Configurability, and Customer success. Please see pages 14 - 15 for more details.
Question 4: Provide an attachment with product literature describing the functionality of the proposed Software. Provide a table that maps your literature with topics listed in this Appendix. Include references to page numbers.	Refer to the attached RFP.
Question 5: Describe the benefits of the technical architecture (i.e. scalability, adaptability, interoperability, etc.).	Being Azure hosted gives FMX the ability to automatically scale rescources automatically so customers are always given the best experience possible.
Question 6: How will the proposed software Solution be accessed (i.e. Web Browser over Internet)?	FMX is a cloud based CMMS. FMX is browser based and can be accessed on any device with a web browser (PC, Laptop, Mobile phone, tablet, etc.) Full functionality is provided on mobile devices and the user interface is tailored to make using FMX on smaller screens a seamless and productive experience. Please see page 20 of the RFP for more information on supported browsers.
Question 7: Describe any additional software that will be required on end-point devices and the access authorization level required to install it.	N/A
Question 8: Describe any add-on or third-party Software required.	N/A
Question 9: Is your product dependent on a solution not included in this proposal?	N/A
Question 10: Describe the degree to which the proposed Solution meets the requirements of RSA chapter 21-R:10, 21-R:11, 21-R:13. https://gencourt.state.nh.us/rsa/html/l/21-R/21-R-mrg.htm	Information included in RFP response.
Topic 2 - USER FRIENDLINESS	
Question 11: How quickly can users perform needed tasks?	FMX is simple and intuitive. Most actions take only a few clicks to complete.

Work Order System Requirements	Additional Comments
Question 12: How easy is it to learn, is it intuitive?	Our approach is simple, it all begins with listening and collaboration. FMX was created based on direct conversations with facilities and maintenance leaders, and that hasn't stopped. Input from professionals like you guides and informs our decisions, so FMX works the way you do.
Question 13: Is its navigation and interface similar to other software used?	Yes, FMX is modern and intuitive to use.
Question 14: How steep is the learning curve?	Implementation and training typically takes 90 days.
Question 15: Please discuss how the solution helps reduce human error.	FMX reduces human error by setting up schedules, alerts, and allowing organizations to input instructions and SOPs to complete tasks.

Topic 3 - ENHANCEMENTS AND NEW RELEASES

Question 16: What types (maintenance, Enhancement, other) of releases are planned?	Routine patches and other enhancements are released weekly. Deployment automation allows us to release a hotfix without taking our website offline. New enhancements are announced closer to lauch of said enhancements.
Question 17: What is the historical (past 3 years) and expected frequency of each type of newrelease?	1-2 times per week.
Question 18: How is the content of future releases determined? Required maintenance, security, userinput?	We use customer feedback, data, and market research to information product releases.
Question 19: Are Enhancements made for specific clients included in future releases for all clients?	Yes, any enhancments made will be availbe to the full customer base.
Question 20: What specific Enhancements are planned for release within the next 24 months?	Our roadmap is planned on our quarterly basis in order to pivot as needed to best serve our customer base.
Question 21: How is the content of a release communicated to the client?	Releases are comunicated via in-app notification, emails, and quarterly product releases on the help desk.
Question 22: Can components of a release be applied individually or by Module without adversely affecting the overall functionality of the System?	This can vary depending on what the release is.
Question 23: How long is a release supported?	N/A: upgrades are automatic.

Topic 4 - DATA IMPORT/EXPORT STANDARDS

NA

Topic 5 - SYSTEM SECURITY

Question 24: Describe the System security design and architectural features incorporated into the proposed Solution

including: | The system incorporates secure design principles, documentation, and testing to protect against hacker attempts throughout the development lifecycle. |

Work Order System Requirements	Additional Comments
Question 25: Compliance with NIST SP 800-171, Protecting Controlled, Unclassified Information in Non- Federal Systems and Organizations	FMX does not specifically follow NIST SP 800 but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
Question 26: Compliance with NIST SP 800-63, Digital Identity Guidelines	FMX does not specifically follow NIST SP 800 but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
Question 27: Compliance with NIST SP 800-115, Technical Guide to Security Testing and Assessment.	FMX does not specifically follow NIST SP 800 but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
Question 28: The methods used to ensure that the parties to interactions with the Application cannot later repudiate or rebut those interactions.	Non-repudiation methods for application interactions include documentation, supervisor review, and disciplinary action.
Question 29: The Intrusion Detection methods used to ensure the detection, recording and review of attempted access or modification by unauthorized individuals.	The system uses intrusion detection systems, physical access mechanisms, and technical testing to protect against unauthorized access and modification.
Question 30: The privacy methods used to ensure that confidential Data and sensitive communications are kept private.	Confidential data is protected through encryption, access controls, and device security measures to ensure privacy.
Question 31: The system maintenance methods used to ensure that system maintenance does not unintentionally disrupt the security mechanisms of the Application or supportinghardware.	Changes are made during off-peak hours and are throroughly reviewed before being implemented.
Question 32: Your Software patch schedule employed to protect the Software from new security vulnerabilities as they arise.	Our policy is to prioritize critical patches for hotfix as soon as possible. The timeline for patching is based on the complexity of the problem, however, 95% of critical patches are released the within 48 hours of problem discovery. FMX also scans and updates third-party libraries for security vulnerabilities.
Question 33: The ability of your Software to be installed in a "locked-down" fashion so as to turn off unnecessary features (user accounts, Operating System Services, etc.) thereby reducing the Software's security vulnerabilities and attack surfaces available to System hackers and attackers.	FMX's software strictly follows the principle of least privelege and allows customers to minutely configure permissions according to that principle.

Work Order System Requirements	Additional Comments
Question 34: The notification and escalation process in the event of an intrusion.	Customers are notified by email as soon as possible when a confirmed data breach is discovered. In addition, the assigned Customer Success Manager will call the customer's primary contact to personally inform them of the situation.
Question 35: What process or methodology is employed within the proposed Software to ensure Data integrity?	We store three copies of all customer data within a primary data center and three copies within a geographically-disparate secondary data center. Additionally, we perform differential database backups every hour, full database backups every week, and we archive database backups for a period of 90 days.
Question 36: To what degree does your approach rely on System assurance capabilities?	Our approach relies on strong system assurance capabilities, including audits and secure system engineering principles.
Question 37: If multiple Databases are employed, what extra procedures are employed to ensure synchronization among Databases?	Extra procedures include redundant storage, load-balanced servers, and synchronized clocks using reputable time sources to ensure data integrity.
Topic 6 - SECURITY TESTING	
Question 38: Describe the testing tools and methodologies used for testing the security of the Software Application and Hosting environment	In addition to annual pen testing and monthly vulnerability scanning, we use automated and manual testing, owasp top 10 checks, and identical production environment to ensure security.
Question 39: How can you ensure the security and confidentiality of the State Data collected on the system?	Implementing appropriate backup procedures and regularly testing backups and restore capabilities, while also carefully selecting and controlling test data.
Question 40: What security validation Documentation will be shared with theState?	Upon signing an NDA, the state may access FMX's Trust Center via trust.gofmx.com, which includes live updates of the security controls FMX followings, relevant security documentation, FMX's security policies, and FMX's security attestation reports.
Question 41: Do you use internal or external resources to conduct SecurityTesting?	We use a combination of internal and external resources to conduct security testing. We use third parties for annual penetration testing but also complete regular internal security testing via vulnerability scanning, code review, manual and automated testing.
Question 42: Describe in detail the options for Vendor-supplied training. Include a proposed training schedule, training topics, and options for participation (e.g., in-person, webinars, one-on-one, on-line, on-demand) that you would provide.	In-depth training on all necessary workflow items for each training group Training formats available: Webinar, self-service via pre-recorded video, self-service via written training guides

Work Order System Requirements	Additional Comments
Question 43: Describe in detail the Documentation that is available to support the training of users of your proposed Solution. Include help screens, On-line or printable manuals and Knowledge bases. If any of these resources would need to be developed or modified for your proposed Solution include a timeline for their availability. If there are access restrictions on any of this material indicate what those restrictions are.	Refer to the Implementation Section of the RFP (Page 18).

Topic 8 - PREPARATION AND EXPECTATIONS OF STATE STAFF INCLUDING TECHNICAL KNOWLEDGE TRANSFER

Work Order System Requirements	Additional Comments
Question 44: Describe how State staff assigned to the Project Team will be involved throughout the Project, including design meetings, decision making, and scope control.	Refer to the Implementation Section of the RFP (Page 18).
Question 45: Provide an overview of Project Team interactions and dependencies between functions	Customer and FMX will jointly manage the project, and each party will manage its resources. All Customer resources shall be available for the duration of the project. Customer will be responsible for managing all assigned project management tasks.
Question 46: Provide recommendations for State staff requirements to maintain the system after Implementation (skill, # of resources, etc.) Include a worksheet or table identifying State staff resources and the projected number of weekly hours to support the system movingforward.	Refer to the Implementation Section of the RFP (Page 18).
Question 47: The transfer of technical knowledge is important for operations, configuration/development, workflow, business setup, maintenance, and management. Address, training curriculum, training priorities and prerequisites, specific commercial and custom course, and one-on-one learning opportunities for State staff.	Refer to the Implementation Section of the RFP (Page 18).
Question 48: Describe and provide samples of the available Documentation supporting the System. Does the Documentation include technical specifications, troubleshooting tips, technical contact information?	Refer to the Implementation Section of the RFP (Page 18).

Topic 9 - IMPLEMENTATION APPROACH

Work Order System Requirements	Additional Comments
Question 49: Provide one or more feasible Implementation Plans. For each plan provided:	Refer to the Implementation Section of the RFP (Page 18).

Work Order System Requirements	Additional Comments
Question 50: Identify timeframes for major milestones, including timing for discontinuing legacy Systems	Implementation timeline An estimate of launch date based on 60-day maximum Import templates For a list of FMX supported data migrations, please see the Pre-site configuration questionnaire Commit to completing before data review and pre-site configuration meeting Commit to sending data that is in an Excel format to CSM
Question 51: Discuss cost implications of the plan, including implications on maintenance fees and available Implementation options that would lower costs.	Refer to the Implementation Section of the RFP (Page 18).
Question 52: Address the level of risk associated with each plan.	Refer to the Implementation Section of the RFP (Page 18).
Question 53: Why is this the approach you recommend?	Refer to the Implementation Section of the RFP (Page 18).
Question 54: Will the Vendor provide a tool for the State and the Vendor to communicate and share information throughout the Project – i.e., SharePoint, Portal?	Refer to the Implementation Section of the RFP (Page 18).
Topic 10 -TESTING MANAGEMENT	
Question 55: Describe in detail the end-to-end testing methodology you propose for this Project.	All changes to our software must pass a battery of automated tests, manual exploratory tests, and receive approval from management before they are released to our production environment. Testing is conducted in an environment that is identical in configuration to production, but contains no production data.
Question 56: Describe testing tools that will be used as part of the Solution testing. Will these tools be available to the State, or will the State be required to purchase tools?	No testing is required by the state. FMX performs quality and security testing internally.
Question 57: Using the following chart, describe the roles and responsibilities required of Vendor Staff and State Staff, include additional information as needed.	See attached sheet.

Test phase	Vendor Role/Responsibility	State Role/Responsibility	Tools	Timeframe
Management of the testing process	Y	N	SDLC tracking system	Ongoing
Test planning	Y	Y (Acceptance testing only)	SDLC tracking system	Ongoing
Test scenario development	Y	Y (Acceptance testing only)	SDLC tracking system	Ongoing
Data preparation	Y	Y (Acceptance testing only)	SDLC tracking system	Ongoing
System preparation	Y	N	Test environments	Ongoing
Unit testing	Y	N	Source code	Ongoing
System integration testing	Y	N	Source code	Ongoing
User acceptance testing	N	Y	Customer site	Optional upon implementation
System performance testing	Y	N	Test environments	Ongoing
Defect tracking	Y	N	SDLC tracking system	Ongoing

Work Order System Requirements	Additional Comments
Question 58: What support will be provided to prepare State staff prior to and during Acceptance Testing? (Training, user Documentation, staff on site, remote support, etc.)	Refer to the Implementation Section of the RFP (Page 18).
Question 59: Will configured Software be delivered in functional components for State Acceptance Testing?	Yes
Question 60: The State has defined 3 levels of Defect severity. Describe how you will adopt this methodology or provide a mapping to outline your proposed representation of Defect severity.	FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer.
Question 61: What tools will be used to document and track status of suspectedDefects?	FMX uses its own software internally to track defect tickets. FMX uses New Relic and its own internal logging to log application errors. FMX uses ZenDesk to collect customer reports of potential defects.
Question 62: What role will the State play in classification and prioritization ofDefects?	FMX customers play no role in the prioritization of defects but can report potential defects to FMX via support@gofmx.com
Question 63: How quickly will a suspected Defect be investigated and how quickly will the Defects be corrected?	Critical defects are resolved within minutes or hours. High priority defects are resolved either same day or 1-2 business days. Medium priority defects are resolved between 1-5 business days. Low priority defects are resolved between 1-14 business days. Very low priority defects are not under SLA.
Question 64: Provide a sample User Acceptance Test Plan from a completed project as an appendix.	Refer to the Implementation Section of the RFP (Page 18).
Question 65: Will System performance be measured and documented using the State's infrastructure and Data? If yes, how? (Not needed for Hosting?)	No, FMX is cloud-hosted.
Question 66: Outline your methodology for Security and Penetration Testing and provide confirmation that it is NIST SP800-115 compliant.	FMX uses Pensive Security for penetration testing. Pensive security utilizes a four-stage methodology based on nist sp 800-115 for security and penetration testing.

Work Order System Requirements	Additional Comments
Topic 11 - MIGRATION STRATEGY	
NA	

Topic 12 - WORK PLAN, STATUS MEETINGS AND REPORTS	
Question 67: The State sees a Work Plan as essential to reaching a comprehensive agreement with a Vendor. Consequently, the State willseek to refine the proposed Work Plan prior toContract approval with the selected Vendor and to incorporate the refined Work Plan by reference into aContract.	Refer to the Implementation Section of the RFP (Page 18).
Question 68: Provide a preliminary Work Plan depicting tasks, task dependencies, Schedule, milestones/critical events, Deliverables, and payment Schedule. Include the Deliverables outlined in Appendix B (Business/Technical Requirements and Deliverables), appropriate status meetings and Reports, and include other Deliverablesthat you, based on experience, would recommend be developed on this Project.	Refer to the Implementation Section of the RFP (Page 18).
Question 69: Define both proposed Written and Software Deliverables. Include sufficient detail that the State will be able to identify departures from the Plan in sufficient time to seek corrective action. In particular, provide information about staffing.	Refer to the Implementation Section of the RFP (Page 18).
Question 70: Describe all Deliverables to be produced in the Project. Ensure that all Deliverables and milestones are identified in the Work Plan. Identify and discuss the following: a) All assumptions upon which the Work Plan is based. b) Descriptions of recommended roles by activity and time required for both State and Vendor members of the Project Team. c) Assignments of members of the Vendor's team identified by role to specific tasks; and d) Critical success factors for the Project.	Refer to the Implementation Section of the RFP (Page 18).
Question 71: Discuss how this Work Plan will be used and State access to Plan details.	Refer to the Implementation Section of the RFP (Page 18).
Question 72: Discuss frequency for updating the Plan, at a minimum biweekly and for every status meeting. Explain how the State will know whether the project is on schedule, project expenses incurred to date, and within budget.	Refer to the Implementation Section of the RFP (Page 18).

Work Order System Requirements	Additional Comments
Question 73: Define your planned approach to maintaining all project documentation. For example, how will this documentation be available to the State staff (Word Doc, SharePoint, etc.).	Refer to the Implementation Section of the RFP (Page 18).
Question 74: The State believesthat effective communication and Reporting are essential to project success. As reasonably requested by the State, Vendor shall provide the State with information or reports regarding the Project. Vendor shall prepare special reports and presentations relating to Project Management shall assist the State in preparing reports and presentations, as reasonably requested by the State, all at no additional cost to the State.	Refer to the Implementation Section of the RFP (Page 18).
Question 75: Describe your planned project management activities including Introductory and Kickoff Meetings, Status Meetings, Work Plan Updates, and Special Meetings. Discuss frequency, duration, participants, agenda items, etc.	Refer to the Implementation Section of the RFP (Page 18).
Question 76: Describe how you will report Project health to communicate Project status with Stakeholdersand for the early recognition of factors that may result in Project problems requiring special attention.	Refer to the Implementation Section of the RFP (Page 18).
Topic 13 - PROJECT RISK AND ISSUE MANAGEMENT	
Question 77: Provide proposed methodologies for project risk and issue management.	Refer to the Implementation Section of the RFP (Page 18).
Question 78: Discuss State and Vendor responsibilities. The State seeks a clear means to compare planned versus actual status, including percentages, at a sufficiently detailed level to ensure the State can adequately monitor the progress of the Project. Be sure to identify any essential time constraints on State actions. Escalation procedures will be defined in a Contract between the State and the Vendor.	Refer to the Implementation Section of the RFP (Page 18).
Topic 14 - QUALITY ASSURANCE APPROACH	

Work Order System Requirements	Additional Comments
Question 79: Describe the methodology that will be employed to assure that each type of Deliverable is of high quality before submission for State consideration (Written, Software, and Non-Software). Discussion should include but not be limited to: a) Provision for State input to the general content of a Written Deliverable and Non-Software Deliverables prior to production. b) The standard for Vendor internal Review of a Written Deliverable and Non-Software Deliverables prior to formal submission; and c) Testing of Software Deliverables prior to submission for Acceptance Testing.	Please see Market Differentiators section of the RFP.
Topic 15 - HOSTED SYSTEM	
Question 80: Describe the service model being offered. Service is Commercial Off the Shelf Software (COTS), Softwareas-a-Service (SaaS), Platform-as-a- service (PaaS), or Infrastructure-as-a-Services (IaaS). The State requires the service provider to use web services exclusively to Interface with the State of New Hampshire's Data in near Real-Time when possible. Describe any client software or plug-in downloads that may be required. It is preferred the service provider's relevant Data Center(s) are certified to the Federal Information Security Management Act (FISMA) level 3 ATO4 and/or Federal Risk and Authorization Management Program (FedRAMP) CSP5 and have independent annual SOC 2 Type 2 audits performed.	The service model being offered is software-as-a-service (saas) and the service provider must use web services for real-time data access.
Question 81: Provide Certifications and latest audit of the Data Center(s) being used in the Solution offered ·	Microsoft Azure has the following attestations: SOC 1, SOC 2, SOC 3, PCI-DSS, FERPA, ISO/IEC 27001, ISO/IEC 27018.

Work Order System Requirements	Additional Comments
Question 82: If Certifications and audits cannot be provided the service provider will be required to implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Information and Non-Public Information. Such security measures must be in accordance with recognized industry practices such as in the National Institute of Standards and Technology (NIST) Controls 800-53 Rev 4 where applicable. Describe controls including but not limited to: a) Data storage, Data Encryption, Data destruction, Data location, Data handling, b) Business continuity and disaster recovery plan. c) Security incident or Data Breach notification, d) Change control and maintenance, e) Patching and upgrades	Microsoft Azure's certifications and controls are available on their website. FMX's certifications and controls are on trust.gofmx.com .
Question 83: Describe how the service provider will provide compliance to all Federal and State of New Hampshire laws, regulations, statutes, policies, standards, and best practices relevant to internet- based hosting	FMX uses Vanta compliance monitoring to ensure that it follows all relevant security and privacy laws.
Question 84: The State requests regularly scheduled Reporting to the State of New Hampshire. Describe the availability of Reports available to the State including latency statistics, user access, user access IP address, user access history and security logs for all State of New Hampshire files related to this RFP.	Access history of customer sites is visible via the product. FMX does not provide access to its security logs.
Question 85: The State requires the system to be available 24/7/365 (with agreed-upon maintenance downtime), and for the Vendor to provide service to customers as defined in a Service Level Agreement (SLA) which will be developed and agreed to in the Contract phase. The State also requires the service provider to guarantee 99% uptime (excluding agreed-upon maintenance downtime). Describe how you will meet these requirements.	Our system is designed with redundancy and hosted in the public cloud to ensure 99% uptime and quick scalability. we also prioritize critical security patches within slas. You can review uptime statistics at status.gofmx.com
Topic 16 -BACKUP AND RECOVERY	
Question 86: Describe the tools used for Backup and Recovery of Applications and Data.	Backup and recovery are managed by our CSP, Microsoft Azure. Backup cadence is determined by FMX and is recorded earlier in this proposal.

Work Order System Requirements	Additional Comments
Question 87: Describe timelines for scheduled backup of Data and Servers including the retention schedule	We store three copies of all customer data within a primary data center and three copies within a geographically-disparate secondary data center. Additionally, we perform differential database backups every hour, full database backups every week, and we archive database backups for a period of 90 days.
Question 88: Describe the impact of the proposed backup process on the operation of the System. Also, address the following:	Backups do not interrupt normal use of the software
Question 89: Use of and method for logging and journaling.	Azure Log Analytics, Azure Storage, Azure Monitor, Azure Defender for Endpoint/Cloud
Question 90: Single points of failure and recommended approaches for their elimination.	Not applicable
Question 91: Approach to redundancy including backup material securely transferred from the site to another secure 25 location to avoid complete Data loss with the loss of a facility.	Data backups are stored in a geographically redundant and encrypted off-site location to prevent data loss in case of a facility failure.
Question 92: Explain your high-level methodology for creation of a Disaster Recovery Plan.	Our high-level methodology includes annual testing and consideration for both operational and information security continuity. More information is available at trust.gofmx.com
Question 93: Discuss how the disaster recovery plan identifies appropriate methods for procuring additional hardware in the event of a component failure. Also describe any impact of Software License fees. The State believes that additional Software License fees solely related to redundancy for Backup and Recovery would be inappropriate. If the Proposal differs from this standard, describe, and provide rationale for the difference.	Data backups are stored in a geographically redundant and encrypted off-site location to prevent data loss in case of a facility failure. This ervice is included in all licenses.
Question 94: Discuss how the disaster recovery plan addresses the recovery of lost State Data as well as your own.	The goal of the disaster recovery plan is to recover all possible data, including FMX customer data.
Question 95: Will the Solution include the option to have the collected Data stored at the Vendor's site, at the State site or both?	No, data is stored in Microsoft Azure's datacenters
Question 96: Provide a plan for business continuity if a disaster occurs at the Data center that is Hosting the proposed Solution	FMX's disaster recovery plan is available for download at trust.gofmx.com
Topic 17 - SUPPORT AND MAINTENANCE FOR VENDOR HOSTED SYSTEM	

Work Order System Requirements	Additional Comments
Question 97: Describe how the System hardware, Software, and Database will be maintained in accordance with the Specifications, terms, and conditions of the RFP, including providing upgrades and fixes as required.	FMX uses Microsoft's PaaS model. Azure is responsible for providing available and up-to-date hardware. Software is maintained by FMX and regularly maintained and updated. Software patches and upgrades are released 1-2 times per week.
Question 98: Describe the Help Desk Support that will be available to State staff including hours of operation, phone vs Email, access to technical support staff.	Refer to Ongoing training and support resources on page 28 in the RFP.
Question 99: Describe the classification of a Software Defect (bug) that will be used to indicate the degree of negative impact on the quality of thew Software and anticipated response times.	FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer. Critical defects are resolved within minutes or hours. High priority defects are resolved either same day or 1-2 business days. Medium priority defects are resolved between 1-5 business days. Low priority defects are resolved between 1-14 business days. Very low priority defects are not under SLA.
Question 100: Describe any particular procedures required to handle escalation and emergency calls.	<u>Emergency calls are handled by following the formal incident response plan, which is reviewed and tested annually. FMX's incident response plan can be found at trust.gofmx. com</u>
Question 101: Detail the types and frequency of support tasksrequired.	FMX's Customer Support service works with customers to troubleshoot defects. For critical, multi-spanning availability or intrustion issues, FMX provides a post-mortem.
Question 102: Describe any different levels and or models of support and maintenance that you provide	FMX's Customer Support service works with customers to troubleshoot defects. For critical, multi-spanning availability or intrustion issues, FMX provides a post-mortem.

Work Order System Requirements	Additional Comments
Question 103: Describe how the Vendor will work with the State to identify and troubleshoot potentially large- scale System failures or Deficiencies by collecting the following information: a) mean time between Reported Deficiencies with the Software; b) diagnosis of the root cause of the problem; and c) identification of repeat calls or repeat Software problems.	FMX's Customer Support service works with customers to troubleshoot defects. For critical, multi-spanning availability or intrustion issues, FMX provides a post-mortem.
Question 104: For all maintenance service calls, the Vendor shall ensure the following information will be collected and maintained: a) nature of the Deficiency; b) current status of the Deficiency; c) action plans, dates, and times; d) expected and actual completion time; e) Deficiency resolution information; f) Resolved by; g) Identifying number i.e. work order number; and h) Issue identified by.	FMX supports configurable fields, so that customers may manage and store additional information within the system.
Question 105: Describe how the State will be informed of emergency maintenance or system outages?	The state will be informed of emergency maintenance or system outages through status.gofmx.com and other regular channels, including email, phone, and meetings.
Question 106: Describe how the Vendor will ensure all hardware and Software components of the Vendor Hosting infrastructure will be fully supported by their respective manufacturers at all times. All critical patches for Operating Systems, Databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	Vendor will ensure timely application of critical patches to all systems and applications, following industry standard configuration and hardening procedures.

Bidder Qualifications

Year Business Started:	2012
State of Incorporation	Ohio
Location of Headquarters	800 Yard St #115, Grandview Heights, OH 43212
Employee Count	140
Ongoing Litigation	None/NA.
Presence in the state of New Hampshire	FMX has 10 customers in the state of New Hampshire.
Identification of which services are provided via the bidder	All services listed in the RFP are provided via FMX.
Sub-contractor including company name, address, contact person, and three references for clients they are currently servicing	No sub-contractors/NA.

Company Information & Experience

Our company history and experience

"I began my career as a mechanical engineer for an energy company and quickly realized that I wanted to make a more strategic impact on the business. It wasn't until 2012, when I was working on an energy conservation project with one of my partners that I realized the need for FMX.

"At the time, the school we were working with was trying to find a way to manage their facilities remotely while maximizing energy savings easily. We began searching for software that was capable of scheduling preventive maintenance, streamlining event scheduling, and tracking maintenance requests. While many options were available, none helped us achieve our needs and were far too complicated for staff members to use on a daily basis.

"We knew we could create something better, so we did."

- Brian Gregory, Founder and CEO of FMX

The platform that Brian and his team created allows facilities leaders to streamline their maintenance processes, increase asset productivity, and track, manage, and improve the metrics that matter most to them. The solution has helped more than 1400 organizations, across K-12, Higher Education, Municipalities, and others, to optimize their operations and reach their facilities and maintenance goals.

FMX is recognized as one of the most-reviewed and highest-rated CMMS providers based on usability and customer satisfaction.

We rely on facilities and maintenance leaders to guide the future of FMX. Their insights influence our product so heavily that we brought a few of these experts onto the team. Together, they have a combined 43 years of experience. These include:

John Bailey, Ph.D.
- National Director, K-12 Business Development
- Former CEO & Executive Director, National School Plant Management Association
- 34 years of experience in the K-12 field as a teacher, principal and director of operations of two large urban school divisions

Darin Porter
- FMX Manager of Industry Practice
- Former K-12 Facilities Manager
- Former FMX customer

Robert Kleimenhagen
- Former Facilities/Operations Director in K-12
- Former Facilities/Operations Director in Municipalities

Matt Pace
- FMX K-12 Practice Leader
- Former K-12 Director of Maintenance and Operations
- Former FMX customer

Tyler Cantrell
- FMX Solutions Engineer
- Former K-12 IT Leader
- Former FMX customer

References

City of Dublin (Ohio)
Matt Earman, Director of Parks and Recreations
mearman@dublin.oh.us
614-348-1588

Eastern State Penitentiary Historic Site
James Travis LII, Associate Director of Design and Facilities
jt@easternstate.org
(215) 236-5111 x221

U.S. Department of Agriculture
Chris Mehelis, Quality Assurance Specialist
chris.mehelis@ars.usda.gov
(510) 559-5697

Vendor Staff Qualifications

FMX's Customer Success leaders have over 30 years of combined experience working with over 1400 organizations to ensure they are deriving value from FMX.

Vice President, Customer Success - Brandi Templeton

Brandi has been with FMX for 8 years. Brandi has previously served as a member of the technical support team as a Customer Success Specialist, a member of the implementation team as a Customer Success Manager, and as a Director of the department. Brandi is now the Vice President of the Customer Success team here at FMX. Brandi's primary responsibilities include providing direction and leadership toward the achievement of the department's goals for customer onboarding, customer satisfaction, renewals, upsells, and Net Promoter Scores (NPS).

Director, Customer Success - Lindsey Dittmar

Lindsey has been with FMX for over 7 years. Starting at FMX in 2017, she learned the ins and outs of the software in a customer support role. Since then, she has been a Customer Success Manager, an Enterprise Customer Success Manager, Manager of the Customer Success team, and now is the Director of Customer Success. Lindsey and her team focus on training and implementing new customers to set them up for success within FMX.

Senior Director, Customer Success - Kathryn Moore

Kathryn has been with FMX for over 8 years. She joined the FMX team in July 2016 as a Customer Success Specialist, working on data migrations and customer support tickets. Afterward, she worked as a Customer Success Manager and Enterprise Customer Success Manager implementing new customers for almost two years until transitioning into Management in the Customer Success department in 2018. Since October 2019, Kathryn has managed the Account Manager team in Customer Success. Kathryn and her team focus on supporting ongoing customers and their ever-changing needs to continue delivering the value of FMX.

Lead, Enterprise Account Manager - Andrea Lindenmuth

Andrea has been with FMX for just over 6 years. As an Enterprise Account Manager, Andrea focuses on being the point of contact for her accounts to ensure they are deriving value from FMX post-implementation. Andrea has been working directly with customers for the last 4 years to ensure customer satisfaction.

Enterprise Account Manager - Emily Rowling

Emily has been with FMX for 4 years. As an Enterprise Account Manager, Emily focuses on being the point of contact for her accounts to ensure they are deriving value from FMX post-implementation. Emily has been working directly with customers for the last 4 years to ensure customer satisfaction.

Implementation

FMX provides these FMX Implementation Requirements to customers prior to the beginning of the implementation process. This document outlines the project assumptions, checkpoints, and meetings throughout the implementation process. After working through over 1,000 implementations, these are FMX's recommended best practices to ensure optimal success with your chosen FMX solutions.

Project assumptions

The following assumptions define the project's full scope and the parameters of what is in-scope and out-of-scope.

- Sufficient and appropriate Customer resources set forth need to be available during the project (for both onsite and remote work).
- Customers will provide a point of contact (e.g., project manager) who is empowered to make decisions and approve direction. This resource will be available at least once each week to meet, review progress, provide feedback and guidance. Customer needs to communicate regularly with FMX and provide FMX with timely feedback.
- Customer and FMX will jointly manage the project, and each party will manage its resources. All Customer resources shall be available for the duration of the project. Customer will be responsible for managing all assigned project management tasks. Client's IT team will be responsible for the Single Sign-On (SSO) setup.

Project team composition

FMX will provide the following resources during implementation:

Role	Description
Customer Success Manager	Responsible for project oversight and collaboration with client project management team, FMX site configuration, oversight of mass data importing, and client training.
Customer Success Specialist	Responsible for mass data importing, SSO login button configuration, existing integration configuration.

| Account Manager | Responsible for the management of client projects post-launch and sharing FMX product innovations. |

Customer will provide the following resources during implementation:

Role	Description
Implementation POC(s)	Responsible for project oversight, resource management, stakeholder interactions and liaison, existing process flows, setup, configuration, and customization of the FMX workflows
Process Owners/Stakeholders	Responsible for participating in requirements gathering, prioritizing requirements
FMX Administrators	Responsible for participating in existing process plows, setup, configuration, and customization of the FMX workflows, daily administration of FMX post-launch.

Data importing

An organization's data on buildings, assets, etc., are the building blocks of an FMX site. Some data is required to use FMX, while other data is optional. Depending on Customer's workflow and reporting needs, some optional data may be needed during the initial implementation. All required data will need to be provided from the Customer to FMX within 7 days of the kickoff meeting in one of the acceptable formats listed below before the Admin Training.

Required data:

- Buildings
- Users

Optional data (may be required depending on Customer's workflow and reporting needs):

- Locations/Resources

- Equipment
- Inventory
- Historical Work Requests
- Historical Planned Maintenance
- Historical Schedule Requests

The following are acceptable data import formats:

- Excel format (cannot be a converted image or PDF file)
- Comma Separated Value (CSV)
- SQL backups
- JavaScript Object Notation (JSON)

The following formats are not acceptable data migration formats:

- Attachments
- PDF files
- Scanned copies
- Paper copies
- Floppy discs

Other free services provided by FMX during initial implementation (additional fee-based services are available after the initial implementation):

1. Data migration from another system

- Transferring data from other software to FMX. To complete this data migration
- FMX will need:
  - Ability to access other software system(s)
  - Data in an Excel, CSV, or other acceptable format from the list above

2. Form Configuration

- FMX will create your request forms for you. To complete the form configurations
- FMX will need a copy of Customer forms. These can be in Excel, CSV, Word, or PDF files.

Timelines for services*:

Type of service	Standard due dates (business days)
Data migration from another system	30
Data import	Up to 15
Form configuration	10

*Timeline for services is dependent on Customer providing and communicating timely with FMX

Single sign-on (SSO)

FMX provides a support agent to enable the SSO feature for FMX. FMX does not configure the SSO database for your organization. FMX supports the following protocols for SSO:
- WS-Federation
- Google OAuth
- SAML-P

Supported browsers

The following are a list of FMX supported browsers:
- Google Chrome (recommended) – Version 50+
- Mozilla Firefox – Version 4+
- Apple Safari – Version 5.1+
- Microsoft Edge – All Versions
- Microsoft Internet Explorer* - Version 11+

*Please note: While we support Internet Explorer, for the best FMX experience, we suggest using one of the other 4 browsers, as well as keeping your web browser updated.

Remote access

FMX is browser based and can be accessed on any device with a web browser (PC, Laptop, Mobile phone, tablet, etc.) Full functionality is provided on mobile devices and the user interface is tailored to make using FMX on smaller screens a seamless and productive experience. On mobile devices FMX also incorporates a barcode scanner that can be utilized to look up information, or assign equipment or inventory to work orders.

Limitations on data storage

There are no limitations on data storage in FMX other than the file size limitation mentioned above. FMX does not limit the total amount of data stored in the system and will store data indefinitely barring the cancellation of a contract. In the event a client decides to cancel their contract with FMX, all data can be exported to excel or csv.

Meeting and process through launch

Meetings and Processes Through Launch	Estimated Days (Recommended)
Kickoff Meeting	Day 0
Data Review and Pre-Site Configuration • Data Input • Pre-Site Configuration • Single Sign-On (SSO)	Days 1-7
Admin Training • Data review • Workflow review • Admin settings review	Days 8-14
Training • Staff Training • Launch	Days 15-21
Post-Launch • One Month Post Launch	Day 21
Total	21 Days

Implementation timeline

- FMX's recommended 21-day implementation is shown for example purposes. FMX's implementation package includes a maximum term of 60 days. If implementation is not completed in 60 days, implementation will be reevaluated and the customer may be subject to an additional fee.
- The Services are provided in increments of full days and reviewed in each implementation meeting.
- All implementation and support work time is based on the FMX standard work schedule of Monday through Friday (8:00 am to 6:00 pm Eastern Time).

- Launch support will be provided as needed, including help from an FMX Customer Success Manager and Customer Success Specialist during their standard work schedule.
- The work will be performed remotely from FMX offices unless otherwise indicated. FMX will bill the travel and expense separately if onsite work is requested.

Definition of terms

- **POC** – Point of contact
- **CSV** - Comma Separated Value
- **JSON** - JavaScript Object Notation
- **SSO** – Single sign-on, or an authentication process that allows a user to access multiple applications with one set of login credentials
- **URL** – Universal resource locator, or the address of a World Wide Web page
- **QBR** – Quarterly business review
- **CS** – Customer Success
- **T&E** – Travel and expense

Kickoff meeting outline

Process	Steps	Resources	Commits & deliverables from FMX	Commits & deliverables from customer
	- Begin the FMX implementation - Project lead introductions - Establish desired outcomes - Develop a Launch Plan - Implementation overview - Introduction to Data Importing	**FMX participants:** Customer Success Manager **Customer participants:** Implementation POC(s), Process Owner(s)/Stakeholder(s), FMX Administrator(s)	**Kickoff PowerPoint** - FMX URL - CSM and FMX Support Contact Info - Meeting Dates **Implementation timeline** An estimate of launch date based on 60-day maximum **Import templates** For a list of FMX supported data migrations, please	**Pre-site configuration questionnaire** Commit to completing before data review and pre-site configuration meeting **Data** Commit to sending data that is in an Excel format to CSM **Training dates** Commit to having

			see the appendix below.	training dates before data review and pre-site configuration meeting
			Pre-site configuration questionnaire CSM to provide a link to a questionnaire	
			SSO documentation FMX to provide documentation for SSO configuration	

Data review and pre-site configuration meeting outline

Process	Steps	Resources	Commits & deliverables from FMX	Commits & deliverables from customer
Data Input	• Learn more about manual and mass data importing **Mass data importing** • Correlation of fields between previous system export and FMX • Confirmation that FMX has all the needed resources to proceed with mass data import	**FMX participants:** Customer Success Manager,Customer Success Specialist **Customer participants:** Implementation POC(s), FMX Administrator(s)	**Import templates and completion of data import** For a list of FMX supported data migrations, please see the appendix below.	**Manual data collection** Commit to gathering any building, location, equipment, inventory, or user information not included in data transfer and needed for the first value **Data import** Commit to sending data that is in an Excel format to CSM
Pre-site configuration	• Review of pre-site configuration questionnaire • Further discussion of desired workflow	**FMX participants:** Customer Success Manager **Customer**	**Site configuration** • User types • Approval process • Request types	**Forms/documents** Commit to sending any forms or documents for configuration to

	processes to be configured within FMX per module	**participants:** Implementation POC(s), FMX Administrator(s)	• Equipment and inventory types • Forms • Misc. feature configuration	CSM
SSO	• Customer to provide FMX with fully configured metadata document or URL		**SSO enabled on FMX site** • For a list of SSO options that FMX supports, please see the appendix below. • **NOTE:** FMX is not a consultant for configuring SSO services on your server.	**Metadata document/URL** Commit to sending metadata document/URL to CSM

Admin training meeting outline

Process	Steps	Resources	Commits & deliverables from FMX	Commits & deliverables from customer
Data review	• Review data questions as needed • Review of imported data to ensure accuracy	**FMX participants:** Customer Success Manager, Customer Success Specialist **Customer participants:** Implementation POC(s), FMX Administrator(s)	• Data import Process Complete • Solidification of the launch date • "Welcome to FMX!" email template	**Data import** Completion of data imports • Training plan to Choose a method for staff training and dates as necessary **NOTE:** All training is held remotely via a Zoom webinar session. Solidification of the launch date

Workflow review	• In-depth training on all aspects of workflow discussed in the previous meeting • Site to be viewed from all needed user types	**FMX participants:** Customer Success Manager **Customer participants:** Implementation POC(s), FMX Administrator(s)	• Workflow knowledge • FMXpert tip	
Admin settings review	• Brief training on the Admin Settings menu of FMX and all tabs involved	**FMX participants:** Customer Success Manager **Customer participants:** Implementation POC(s), FMX Administrator(s)		

Training meeting

Process	Steps	Resources	Commits & deliverables from FMX	Commits & deliverables from customer
Staff training	• In-depth training on all necessary workflow items for each training group • Training formats available: Webinar, self-service via pre-recorded video, self-service via written training guides	**FMX participants:** Customer Success Manager **Customer participants:** Implementation POC(s), Training groups	• Training videos • CSM to provide a link to training videos	
Launch	"Welcome to FMX!" email is sent to all staff	**Customer participants:** Implementation POC(s), FMX Administrator(s)	**First value** CSM to ensure Customer has started receiving value from FMX	**Launch FMX site** Commit to having staff begin submitting requests

Post-launch meeting

Process	Steps	Resources	Commits & deliverables from FMX	Commits & deliverables from customer
One Month Post-Launch	• Introduction to Account Manager • Revisit the desired outcomes stated during the Kickoff meeting • Review product modules • Identify new pain points • Set new goals and desired outcomes • Review new FMX features • Set regular Business Review cadence	**FMX Participants:** Customer Success Manager, Account Manager **Customer Participants:** Implementation POC(s), Process Owner(s)/Stakehol der(s), FMX Administrator(s)	BR PowerPoint	Attendance at One-Month Post-Launch Meeting

Ongoing training and support resources

Upon completion of implementation, FMX will assign a designated Account Manager for your school district. This contact will be the main FMX delegate for your school district throughout the lifetime of our relationship.

FMX offers a variety of training videos and support articles on our support center which can be found on our website as well as by clicking the "Help and Updates" link on the FMX application.

Additionally, ongoing training is included in the event the district requires additional training for new staff or refresher training to ensure proper utilization of FMX.

Support availability and timing

FMX support is available Monday through Friday from 8 am to 6 pm ET. Contact options include email (support@gofmx.com) and phone (844.644.4400). You can also schedule remote meetings with your AM by contacting them at their direct line or email.

Pricing

Pricing Proposal

Below you will find our pricing proposal for this RFP. Pricing is based on 95 licensed users (70 technicians, 20 primary users and 5 administrators.)

Hosted Software License Name	Year 1	Year 2	Year 3	Year 4	Year 5
Maintenance Requests, PMs, Reporting	$52,800	$52,800	$52,800	$55,440	$58,212
Total	$52,800	$52,800	$52,800	$55,440	$58,212

Hardware Item	Unit Cost
Barcode Scanning Gun	N/A
Barcode Printer	$0
*There is no barcode scanner needed. You can use your smartphone or tablet	
Total	$0

Other Cost Description	Year 1	Year 2	Year 3	Year 4	Year 5
Implementation and Training	$26,400	$0	$0	$0	$0
Total	**$26,400**	**$0**	**$0**	**$0**	**$0**

Bidder Contact Information:

Name: Ameshia Williams
Email: ameshia.williams@gofmx.com
Phone Number: (585) 705-7885

Company Website: www.gofmx.com
Company Name: FMX
Company Address: 800 Yard Street Columbus, Ohio 43212
DUNS: 079858910

APPENDIX F - VENDOR RISK ASSESSMENT REPORT (VRAR)

VENDOR SYSTEM INFORMATION: *Table 2.1 System Information*

VENDOR Name:	Facilites Management eXpress LLC.
Solution/System Name:	FMX
Service Model: (e.g., IaaS, PaaS, SaaS)	SaaS
FIPS PUB 199 System Security Level: (e.g., Moderate, Low)	Low
Fully Operational as of: Enter the date the system became fully operational.	FMX was founded in November, 2012.
Number of Customers (State/Others): Enter # of customers / # of other customers	FMX has roughly 2000 customers
Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only	Yes, our service is a Public Cloud deployment model.
Cloud, or Other? If other, please describe.	We use Microsoft Azure as our cloud service provider and maintain control of patches and changes to our application and database service.
System Functionality: Briefly describe the functionality of the system and service being provided.	FMX is a an easy to use and configurable CMMS with modules to manage work orders, preventive maintenance, assets, equipment. FMX also has comprehensive reporting so organizations can gather actionable insights to save time, money, and more.

Table 2.2 Leveraged Systems

Is this system leveraging an underlying provider?	No, all FMX products are developed by FMX. FMX does use Microsoft Azure as its CSP.

Table 2.2 Leveraged Systems

State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.	None

Table 2-4. System Interconnections

Does the system connect to the internet?	Yes
Does the system connect to a corporate or state infrastructure/network?	No
Does the system connect to external systems?	Possibly, depending on the customer's chosen configuration.

Compliance Topic

#		
1	1 Data at Rest, Authentication: Are only FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules used where cryptography is required?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
2	2 Transmission, Remote Access: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
3	3 Can the VENDOR'S solution integrate with the State's IAM solution(s)?	FMX has an open API, more details can be provided upon request.
4	4 Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application...e.g., firewalls intrusion detection/ prevention systems, end point protection etc.? [SC-7] [SI-3/SI-4]	Yes, the VENDOR uses security boundary/threat protection devices such as firewalls, intrusion detection/prevention systems, and endpoint protection.
5	5 Can the VENDOR consistently remediate High risk vulnerabilities within 30 days and Medium risk vulnerabilities within 60 days? [SI-2]	Yes
6	6 Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?	Yes, our data backup and retention policies comply with all relevant legal and regulatory requirements, including HIPAA, NARA, and FOIA.
7	7 Does the VENDOR store, process or transmit State data only in the continental US and is that data backed up in only US locations?	Yes, all data is stored and backed up within the US and encrypted at rest in geographically redundant locations.
8	8 Does the VENDOR have a process to securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 and will provide to the State a certificate of data destruction? [MP-6]	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls. We will provide the State a certificate of data deletion if requested. Data destruction is obfoscated from us and managed by Microsoft Azure.
9	9 All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement?	The OS layer of our application is managed via Microsoft Azure
10	Does the vendor have a current 3rd party attestation certification and is it regularly renewed? The State desires an independent 3rd party attestation (e.g., FedRAMP, StateRAMP, SOC 2 Type 2, ISO 27001, or HITRUST) prior to contract award for systems containing Restricted/Highly Restricted data. Note: SaaS vendors covered as part of the IaaS/PaaS assessments, [CA-7, RA-3, SA-9]cannot use IaaS/PaaS certification unless the application is explicitly	Yes, our company has undergone a SOC 2 Type 1 and is actively pursuing a SOC 2 Type 2.
11	Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to Federal and/or State Restricted/Highly Restricted regulations and procedures for those systems that require it? [AC-2, PS-3]	Yes, the VENDORs staff undergoes appropriate background checks for unprivileged and privileged access, in accordance with Federal and/or State regulations and procedures.

Table 3-2a. Data at Rest & Authentication

#		
1	Data at Rest [SC-28]; FIPS 140-2 Validated?; NSA Approved?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
2	Authentication [IA-5, IA-7]; FIPS 140-2 Validated?; NSA Approved?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.

Table 3-2b. Transport Encryption

#		
1	Transmission [SC-8 (1), SC-12, SC-12 (2, 3)]; FIPS 140-2 Validated?; NSA Approved?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.
2	Remote Access (AC-17 (2)]; FIPS 140-2 Validated?; NSA Approved?	FMX does not specifically follow FIPS but does follow SOC 2 controls, which are based in part of NIST controls. FMX's hosting provider, Microsoft Azure does follow NIST SP 800 controls in addition to many other security controls.

Table 3-4. Identification and Authentication, Authorization, and Access Control

#		
1	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation? [IA-2, IA-4]	Yes, the system uniquely identifies and authorizes organizational users in a way that reduces the risk of impersonation.

2	2 Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2 (1), IA-2 (2)]	Yes, MFA can be required for all administrative accounts and functions, including remote access for third-parties via the use of SSO integration.
3	3 Is role-based access used, managed, and monitored? [IA-4, IA-5]	Yes, role-based access is used, managed, and monitored through structured rules and additional security controls.
4	4 Does the system restrict non-authorized personnel's access to resources? [AC-6, AC-6 (1), AC-6 (2)]	Yes, the system restricts non-authorized personnel's access to resources through access controls and procedures.
5	5 Does the system restrict non-privileged users from performing privileged function? [AC-6, AC-6 (1), AC-6 (2), AC-6 (10)]	Yes, the system restricts non-privileged users from performing privileged functions through user access and role reviews.
6	6 Does the system ensure secure separation of customer data? [SC-4]	Yes, customer data is securely separated and managed in accordance with relevant regulations and customer agreements.
7	7 Does the system ensure secure separation of customer processing environments? [SC-2]	Yes, our system ensures secure separation of customer processing environments through strict segregation and approval processes.
8	8 Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2]	Yes, access controls for administrative personnel are based on granular permissions and additional security controls.
9	9 Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]	Yes, the remote access capability must adhere to VENDOR-defined restrictions, configuration guidance, and authorization procedures.
10	10 How will the State's password policy be enforced? State requires minimum 14-character complex passwords (Upper, Lower, Special Character & Numerical) [IA-5]	The State can enforce their password controls via SSO integration.

Table 3-5. Audit, Alerting, Malware, and Incident Response

1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3]	Yes, the system has the capability to detect, contain, and eradicate malicious software through anti-malware protections and threat detection and response software.
2	2 Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-4, AU-9]	Yes, our system stores audit data in a tamper-resistant manner and meets chain of custody and e-discovery requirements.
3	3 Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-4 (5), SI-7, SI-7 (7)]	Yes, the vendor has the capability to detect unauthorized or malicious use of the system through automated monitoring and security personnel.
4	4 Does the VENDOR log and monitor access to the system? [SI-4]	Yes, the system logs and monitors access by specific users, date/time, and originating IP/device for security purposes.
5	5 Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	Yes, Facilities Management Express has a formal incident response plan that is reviewed, tested, and documented annually.
6	6 Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11]	Yes, the vendor performs security code analysis and utilizes various tools to identify and remediate security flaws.
7	7 Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4, IR-4 (1), IR-6]	Yes, the VENDOR implements automated mechanisms for incident handling and reporting through qualified engineers and an incident response team.
8	8 Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-11]	Yes, the vendor retains online audit records for at least 90 days and offline for at least one year.
9	9 Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NH's requirement for security breach reporting is 24 hrs, of incident confirmation. [IR-6]	Yes, the vendor has the capability to notify customers and regulators within 24 hours of confirmed incidents, as required by State of NH.
10	10 If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection?	Yes, the VENDORs solution supports DMARC and DKIM for email protection.

Table 3-6. Contingency Planning and Disaster Recovery

1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-9, CP-10]	Yes, the VENDOR has a disaster recovery plan and conducts an annual test to ensure continuity of information security.
2	2 Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with Statewide Information Security Manual? [CP-2, CP-4]	Yes, however the Statewide Information Security Manual was not used as a reference for this plan.
3	3 Does the system have alternate storage and processing facilities? [CP-6, CP-7]	Yes, the system has alternate storage and processing facilities to meet Facilities Management Express requirements for data protection.
4	4 Does the system have or use alternate telecommunications providers? [CP-8]	the customer has sole control over internet connectivity and is responsible for proper functioning of the system.
5	5 Does the system have backup power generation or other redundancy? [PE-11]	This aspect of the service is managed by Microsoft Azure which does have these capabilities
6	6 Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8]	the customer has sole control over internet connectivity and is responsible for proper functioning of the system.

Table 3-7. Configuration and Risk Management

1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	Yes, the VENDOR maintains a current, complete, and accurate baseline configuration of the information system through regular reviews and updates.
2	2 Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	Yes, the vendor maintains an up-to-date inventory of all software, hardware, and network components in our information system.
3	3 Does the VENDOR have a Configuration Management Plan? [CM-9]	No
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4, CM-4 (2)]	Yes, our formal change control process includes a security impact assessment for all changes before they are moved to production.
5	5 Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2, CM-2 (2), CM-6, CM-8]	Yes, the VENDOR employs automated mechanisms to detect inventory and configuration changes through regular vulnerability monitoring and self-repair/alerting of critical files.
6	6 Does the VENDOR prevent unauthorized changes to the system? [CM-5]	Yes, all changes must comply with Change Management procedures and are only performed by authorized personnel.
7	7 Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6, CM-7]	Yes
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]	No
9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5 (5)]	Yes

10	10 Does the VENDOR demonstrate the capability to remediate High risk vulnerabilities within 30 days and Moderate risk vulnerabilities within 60 days? [RA-5, SI-2]	Yes
	Describe how the Vendor validated that the VENDOR remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 60 days.	Reporting on past tickets
11	11 When a high-risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5]	Yes, the vendor consistently checks audit logs for evidence of exploitation through automated monitoring and manual review.
13	12 Does the VENDOR have a Supply Chain Risk Management (SCRM) plan and processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems?	Not applicable. FMX does not require supplies to be regularly operational.

Table 3-8. Data Center Security

1	Does the VENDOR restrict physical system access to only authorized personnel? (PE-2 through PE-6, PE-8)	This aspect is handled by Microsoft Azure and is part of their service
2	2 Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]	This aspect is handled by Microsoft Azure and is part of their service
3	3 Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6, PE-6 (1)]	This aspect is handled by Microsoft Azure and is part of their service

Table 3-9. Policies and Procedures

Please refer to https://trust.gofmx.com/ for specifics.

Table 3-11. Security Awareness Training

1	Does the VENDOR train personnel on security awareness and role-based security responsibilities? [AT-2]	Yes, the VENDOR provides training for security awareness and role-based security responsibilities to personnel.

Table 3-13. Change Management

1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?	Yes, our change management process includes authorization, impact analysis, testing, and validation before changes are moved to production. Our documented process includes planning, testing, approval, communication, and remediation measures.
1	2 Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	Yes, we have established and followed software testing processes in a production-like environment before promoting changes to production.

Table 3-14. Vendor Dependencies and Agreements

1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?	Yes, Microsoft Azure
2	2 Within the system, are all products still actively supported by their respective vendors?	Yes
3	3 Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?	Yes

Table 3-17. Continuous Monitoring Capabilities

1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	Yes, our lifecycle management plan ensures timely updates and monitoring of vendor support periods for all products.
2	2 Does the VENDOR have the ability to scan all hosts in the inventory?	Yes
3	3 Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML files?	FMX does not share the results of scans to limit the surface area of attack
4	4 Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	FMX maintains a risk assessment and mitigation plan as part of its SOC 2 compliance

Appendix G: Application Requirements

GENERAL SPECIFICATIONS

1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	Yes
2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	Yes
3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	Yes

APPLICATION SECURITY

1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	Yes
2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	Yes
3	Enforce unique user names.	Yes
4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy.	Yes, complex passwords are enforced via SSO integration
5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	Yes, complex passwords are enforced via SSO integration
6	Encrypt passwords in transmission and at rest within the database.	Yes
7	Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy.	Yes, complex passwords are enforced via SSO integration
8	Provide the ability to limit the number of people that can grant or change authorizations.	Yes
9	Establish ability to enforce session timeouts during periods of inactivity.	Yes, session timeouts can be enforced via SSO integration
10	The application shall not store authentication credentials or sensitive data in its code.	Yes

11	Log all attempted accesses that fail identification, authentication and authorization requirements.	Yes, attempted access logs can be enforced via SSO integration
12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	Yes
13	All logs must be kept for (90 days).	Yes
14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	Yes
15	Do not use Software and System Services for anything other than they are designed for.	Yes
16	The application Data shall be protected from unauthorized use when at rest.	Yes, data is protected at rest through encryption using AES 256 and access is restricted to authorized roles.
17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	Yes
18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	Yes
19	Utilize change management documentation and procedures.	Yes
20	Web Services : The service provider shall use Web services exclusively to interface with the State's data in near real time when possible.	Yes

APPLICATION SECURITY TESTING

1	All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	Yes
2	The Vendor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	Yes
3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.	Please see trust.gofmx.com
4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	Yes
5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	Yes
6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	Yes
7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.	Yes
8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	Yes
9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	Yes
10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	Yes
11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	Yes
12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project).	Yes, regular security reviews and adherence to OWASP top 10 are used to mitigate common web application vulnerabilities.
13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	Yes, we perform third-party security reviews using a combination of vulnerability scanning, penetration testing, and code analysis tools. Please see trust.gofmx.com
14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	Please see trust.gofmx.com
15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	Please see trust.gofmx.com

STANDARD TESTING

1	The Vendor must test the software and the system using an industry standard and State approved testing methodology.	Please see trust.gofmx.com for the standards FMX follows
2	The Vendor must perform application stress testing and tuning.	Yes
3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	Not applicable
4	The vendor must define and test disaster recovery procedures.	Yes, our disaster recovery plan is tested annually and includes testing of backup restoration processes and continuity of information security. Please see trust.gofmx.com

OPERATIONS

1	Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%.	FMX uses Microsoft Azure for hosting
2	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	FMX uses Microsoft Azure for hosting
3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	FMX uses Microsoft Azure for hosting
4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	FMX uses Microsoft Azure for hosting
5	Vendor shall monitor System, security, and application logs.	Yes
6	Vendor shall manage the sharing of data resources.	Yes
7	Vendor shall manage daily backups, off-site data storage, and restore operations.	Yes
8	The Vendor shall monitor physical hardware.	FMX uses Microsoft Azure for hosting
9	Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	Not applicable
10	The Vendor shall report any breach in security in conformance with State of NH RSA 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.	Yes

DISASTER RECOVERY

1	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	Yes. Our DRP is tested annually and includes backup restoration processes and continuity of information security and operational continuity. Please see trust.gofmx.com
2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	Not applicable
3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	Yes
4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	Yes
5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	Yes, backups are taken daily and weekly for all servers, with additional hourly backups for SQL servers.
6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	Yes

#	Requirement	Response
7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	Not applicable

HOSTING SECURITY

#	Requirement	Response
1	The Vendor shall employ security measures ensure that the State's application and data is protected.	Yes
2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	Yes
3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	FMX uses Microsoft Azure for hosting
4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	Yes
5	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	Yes
6	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.	Yes, so long as these audits do not interfere with FMX's normal business operations
7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	Yes
8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.	Yes
9	The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.	No, while FMX aims to inform customers of breaches as soon as possible, 2 hours is insufficient time for FMX to understand the impact of a breach if one were to occur and provide a recommendation. FMX will agree to a notification within 24 hours.
10	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	Please review FMX's Terms and Conditions attached

SERVICE LEVEL AGREEMENT

#	Requirement	Response
1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	Yes
2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	Yes, however, Microsoft Azure will maintain the hardware.
3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	Yes, however, Microsoft Azure will maintain the hardware.
4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	Yes, however, Microsoft Azure will maintain the hardware.
5	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff any time of day, seven days per week.	No, FMX's support phone support hours are from 8AM to 6PM EST. The State may email in requests at any time.

#	Requirement	Response
6	The Vendor shall conform to the specific deficiency class as described: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	No, FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer.
7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.	No, critical defects are resolved within minutes or hours. High priority defects are resolved either same day or 1-2 business days. Medium priority defects are resolved between 1-5 business days. Low priority defects are resolved between 1-14 business days. Very low priority defects are not under SLA.
8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	No, FMX will commit to a 99.9% uptime measured yearly. No software solution is without downtime.
9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	Yes
10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	FMX will commit to a 99.9% uptime, measured yearly. This is equivalent to 364.5 days of uptime. If FMX falls short of this number, FMX will comply with the State's uptime credit policy.
11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	Yes
12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	No, FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer.
13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	Yes
14	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	No, this interferes with FMX's normal business operations.

SUPPORT & MAINTENANCE REQUIREMENTS

#	Requirement	Response
1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	Yes
2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	Yes

No.	Requirement	Response
3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	Yes
4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 7:30am to 5:00pm- Monday through Friday EST.	Yes
5	The Vendor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	No, FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer.
6	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	Yes
7	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by; 7) Identifying number i.e. work order number; 8) Issue identified by;	Yes
8	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	Yes
9	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties.	Yes
10	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	Yes
11	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	No, FMX has five defect levels: Critical, High, Medium, Low, and Very Low. Critical represents an availability or intrusion event and is addressed immediately by all hands. High represents the inability for multiple FMX customers to operate standard workflows. Medium represents the inability of one FMX customer to operate standard workflows or multiple FMX customers being only able to operate standard workflows via a workaround. Low represents the inability of one or more FMX customers being unable to operate non-standard workflows. Very Low represents a low defect that is discovered internally but not yet reported by a customer.

12	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	Yes
13	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	Yes
14	The Vendor shall give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	No
15	The State shall provide the Vendor with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	No applicable

PROJECT MANAGEMENT

1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	Yes
2	Vendor shall provide Project Staff as specified in the RFP.	Yes
3	Vendor shall submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, milestones/critical events, task dependencies, and payment Schedule. The plan shall be updated no less than <every two weeks.>	Yes
4	Vendor shall provide detailed <bi-weekly or monthly> status reports on the progress of the Project, which will include expenses incurred year to date.	Yes
5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Define how- WORD format- on-Line, in a common library or on paper).	Yes