mle

200

State of New Hampshire

DEPARTMENT OF ADMINISTRATIVE SERVICES
25 Capitol Street – Room 100
Concord, New Hampshire 03301
Office@das.nh.gov

Charles M. Arlingbaus
Commissioner
(603) 271-3201

Catherine A. Keane
Deputy Commissioner
(603) 271-2059

Sheri Rockburn
Assistant Commissioner
(603) 271-3204

June 17, 2022

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

REQUESTED ACTION

Authorize the Department of Administrative Services (DAS) and the New Hampshire Department of Employment Security (NHES) to enter into a contract with Metropolitan Life Insurance Company (MetLife), 200 Park Avenue, New York, NY (VC #211347) in an amount up to and not to exceed $6,164,665.00 for the purpose of providing the State of New Hampshire with Commercial Insurance Carrier Services for the Granite State Paid Family Medical Leave ("PFML") Plan ("the Plan") in accordance with RSA 21-I:96-108 and RSA 282-B:1-10. This contract shall be effective upon Governor and Executive Council approval through December 31, 2027 with an option to extend for up to an additional two (2) years. 100% General Funds

Funds are available in account 01-14-14-144510-21770000-102-500731 for FY 23 and are anticipated to become available in future operating budgets with the authority to adjust costs and encumbrances between fiscal years within the price limitation through the Budget Office, if needed and justified.

Class	Description	FY23 (6 mths)	FY24	FY25	FY26	FY 27 (6 mths)	Total
102-500731	Contracts for Program Services	$573,461	$1,598,950	$1,676,542	$1,710,073	$605,639	**$6,164,665**

EXPLANATION

The Granite State Paid Family Leave Plan

The Granite State Paid Family Leave Plan (PFML Plan) was established in House Bill 2 (Chapter 91, Laws of 2021) (the law) as a voluntary program that provides participating NH workers with PFML insurance coverage at 60% of their average weekly wage for up to 6 weeks. The PFML Plan is for specific leaves of absence from the workplace associated with the birth of a child, placement of a child for adoption or fostering, a serious health condition of a family member, a qualifying exigency arising from foreign deployment with the armed services or caring for a service member with a serious injury or illness as permitted under the federal Family and Medical Leave Act (FMLA) and for the employee's own serious health condition, if applicable.

The law requires DAS to purchase paid family leave insurance for state workers as a way to create a PFML insurance market in New Hampshire. State employee coverage excludes first person coverage for a state employee's own serious health condition in recognition of the generous, collectively bargained paid sick leave that state employees accrue in addition to the wage replacement benefits that state employees are eligible to receive in the event that they are disabled from performing their job and have exhausted all accrued sick time.

Participation by other public and private sector employers and employees in the Plan is entirely voluntary. Large employers participating in the Plan will contract with and remit payment directly to the carrier. Employers of all sizes may determine the manner in which the PFML insurance coverage they purchase coordinates with their leave policies and/or the federal FMLA. The law provides employers purchasing PFML insurance under the Plan with a business enterprise tax credit in the amount of 50% of the PFML premium paid by an employer for six weeks of PFML coverage. Employers can choose how to structure premium costs by paying the full premium or by passing all or part of the cost along to their employees. Individuals whose employers do not opt into the plan may also participate in the plan.

The law allows individuals whose employers decline to participate in the Plan to purchase PFML insurance by making payments into the PFML Premium Fund administered by NHES. Small employers (< 50 employees) can also participate in the plan by making premium payments into the PFML Premium fund. The law establishes a PFML Premium Stabilization Trust Fund into which the premium taxes on PFML insurance are deposited to create a premium stabilization reserve so that the rates paid by individual participants in the individual purchasing pool do not exceed $5 per week.

RSA 21-I:107 and RSA 282-B:8 contain identical provisions to fund the Granite State Paid Family Leave Plan. Each provision states that "[t]he state treasurer shall transfer funds from the general fund to the [department of administrative services/department of employment security] for the payment of the administrative and implementation costs associated with this chapter." For ease of contract administration and payment of the contractor invoices, the costs of this contract if approved will be administered in the above referenced account established at DAS.

The PFML Plan is a first in the nation voluntary plan that uses the State's purchasing power and tax expenditure authority to provide advantageously priced PFML insurance for NH employers and employees of businesses of all sizes. For employers, the NH PFML Plan promotes the retention and recruitment of workers, enriches their benefit offerings, increases employee satisfaction, morale and productivity, and reduces costs associated with employee turnover. For employees, the NH PFML Plan protects their income and promotes continued attachment to the workforce when they need to take time off from work to care for a family member with a health issue, for the birth and bonding of a new child, or to deal with their own serious health condition. In short, paid family and medical leave can significantly improve employees' lives and businesses' bottom lines.

Paid Family Medical Leave Plan Procurement

On March 28, 2022, the DAS Division of Procurement and Support Services issued a Request for Proposal (RFP) for an insurance carrier to administer the Granite State PFML Plan. DAS sent notifications of the RFP through the appropriate Institute for Public Procurement (NIGP) industry code database. The RFP was also posted on the Division of Procurement and Support Services' public website. On May 9, 2022, two proposals were received, however only the proposal from MetLife met the minimum requirements for acceptance.

The scoring of the proposal was based on the combined score of the Financial (50%) and Non-Financial (50%) components. The Evaluation Team consisted of the following members: Catherine Keane, DAS Deputy Commissioner; Gary Lunetta, DAS Director of Procurement and Support Services; Andrew Bennett, DAS Purchasing Agent; Laura Holmes, DAS Project Manager; Richard Lavers, NHES Deputy Commissioner; Brian Gottlob, Director of the Economic and Labor Market Information Bureau, NHES; Roni Karnis, Life, Annuity & Ancillary Health Legal Counsel, NH Insurance Department; Lisa Cota-Robles, Health Reform Coordinator, Life & Health Division, NH Insurance Department; and Sally Gallerani, Director, Technical Support Services, Department of Information Technology. The Evaluation Team met and unanimously selected MetLife.

Under this five-year contract, MetLife will provide PFML coverage for permanent state employees working in all three branches of state government. The price limitation of this contract represents the cost of the state employee PFML coverage and is based on a five-year, fixed rate that is applied to state employee wages up to the Social Security cap with a 2% escalation per year that is projected to provide room for an increase in the number of permanent state employees (employees with tenure of six or twelve months depending on the branch where employed) and employee wages over the life of the contract. In addition, Metlife is required to offer coverage for purchase to large and small employers through house staff or its network of insurance producers, agents and benefits consultants. Pursuant to this contract and proposed NH Insurance Department administrative rules, employers will be able to customize the PFML coverage they purchase by expanding coverage from six to up to twelve weeks and defining the waiting and elimination periods. Individuals whose employers do not participate in the plan may also voluntarily purchase coverage under the Plan, and in accordance with the law, their premium costs may not exceed $5 per week. This contract requires Metlife to provide a website that is available 24/7 and a contact call center that is available from 8 am to 11 pm Eastern Time. Finally, Metlife is required by this contract to provide the state with reporting on plan participation and other metrics and to work with the state and its marketing vendor to educate employers and the public about the plan.

After selecting MetLife as a bidder, the DAS Division of Procurement and Support Services entered into negotiations with the bidder. MetLife agreed to reduce its pricing for coverage for state employees by 10% over the five-year contract from $1,369,925.55 to $1,232,933.00 resulting in savings of $684,962.77.

Based on the foregoing, we are respectfully recommending approval of the contract.

Respectfully Submitted,

Charles M. Arlinghaus

Charles M. Arlinghaus
Commissioner
Department of Administrative Services

George N. Copadis
Commissioner
NH Employment Security

Division of Procurement Support Services
Bureau of Purchase Property

Gary S. Lunetta
Director
(603) 271-2201

RFP Description	Commercial Insurance Carrier for the Granite State Paid Family and Medical Leave Plan	Agency:	Statewide
RFP #	2571-22	Requisition: #	N/A
Agent Name	Andrew Bennett	RFP Closing:	5/9/22 @ 10:00 AM

Vendor		**Total Score**
Metropolitan Life Insurance Company		**919**
Indicates highest score		

FORM NUMBER P-37 (version 12/11/2019)

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 and NH Employment Security		1.2 State Agency Address 25 Capitol Street, Room 102 Concord, NH 03301	
1.3 Contractor Name Metropolitan Life Insurance Company		1.4 Contractor Address 200 Park Avenue 6th Floor New York, NY 10166	
1.5 Contractor Phone Number 617-529-8215	1.6 Account Number Multiple	1.7 Completion Date December 31, 2027	1.8 Price Limitation $6,164,665.00
1.9 Contracting Officer for State Agency Director Gary Lunetta Procurement and Support Services		1.10 State Agency Telephone Number 603-271-2201	
1.11 Contractor Signature David S. Brennan Date: 6/17/2022		1.12 Name and Title of Contractor Signatory David S. Brennan, Vice President	
1.13 State Agency Signature Date: 6/17/22		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: Takhmina Rakhmatova On: 6/17/2022			
1.17 Approval by the Governor and Executive Council *(if applicable)* G&C Item number: G&C Meeting Date:			

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 as indicated in block 1.17, 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. 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 affected 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. 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, 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 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. The State shall have no liability to the Contractor other than the contract price.

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 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.

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. 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 race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.

6.3. 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 all rules, regulations and, orders, and 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 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.

7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State's representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer's decision shall be final for the State.

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) days from the date of the notice; and if the Event of Default is not timely cured, terminate this Agreement, effective two (2) 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.

8.3. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

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) 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) 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. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT B. In addition, at the State's discretion, the Contractor shall, within 15 days of notice of early termination, develop and submit to the State a Transition Plan for services under the Agreement.

10. DATA/ACCESS/CONFIDENTIALITY/ PRESERVATION.

10.1 As used in this Agreement, the word "data" shall mean all 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 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data 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 The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written notice, which shall be provided to the State at least fifteen (15) days prior to the assignment, and a written consent of the State. For purposes of this paragraph, 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.

12.2 None of the Services shall be subcontracted by the Contractor without prior written notice and consent of the State. 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. Unless otherwise exempted by law, the Contractor shall indemnify and hold harmless the State, its officers and employees, from and against any and all claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement, or other claims asserted against the State, its officers or employees, which arise out of (or which may be claimed to arise out of) the acts or omission of the Contractor, or subcontractors, including but not limited to the negligence, reckless or intentional conduct. 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 sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

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 his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than ten (10) days prior to the expiration date of each insurance policy. 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 his or her 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. 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.

17. 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.

18. CHOICE OF LAW AND FORUM. This Agreement shall be governed, interpreted and construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. 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. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

19. CONFLICTING TERMS. In the event of a conflict between the terms of this P-37 form (as modified in EXHIBIT A) and/or attachments and amendment thereof, the terms of the P-37 (as modified in EXHIBIT A) shall control.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. 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.

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

23. 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.

24. 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.

TABLE OF CONTENTS

Contractor Initials QB
Date 6/17/2022

10. DATA/ACCESS/CONFIDENTIALITY/ PRESERVATION.
Delete Provision 10.2 in its entirety and replace with the following:
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 pursuant to MetLife's records retention policy, and any applicable law.

13. INDEMNIFICATION.
Delete Provision 13 Indemnification in its entirety and replace with the following:
Unless otherwise exempted by law, the Contractor shall indemnify and hold harmless the State, its officers and employees from and against any and all third-party claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement, or other claims asserted against the State, its officers or employees, which arise out of the acts or omission of the Contractor, or subcontractors, in respect to any services provided under this agreement and in connection with the benefits made available through the State of New Hampshire to employees of the State, including but not limited to the negligence, reckless or intentional conduct. 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 sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

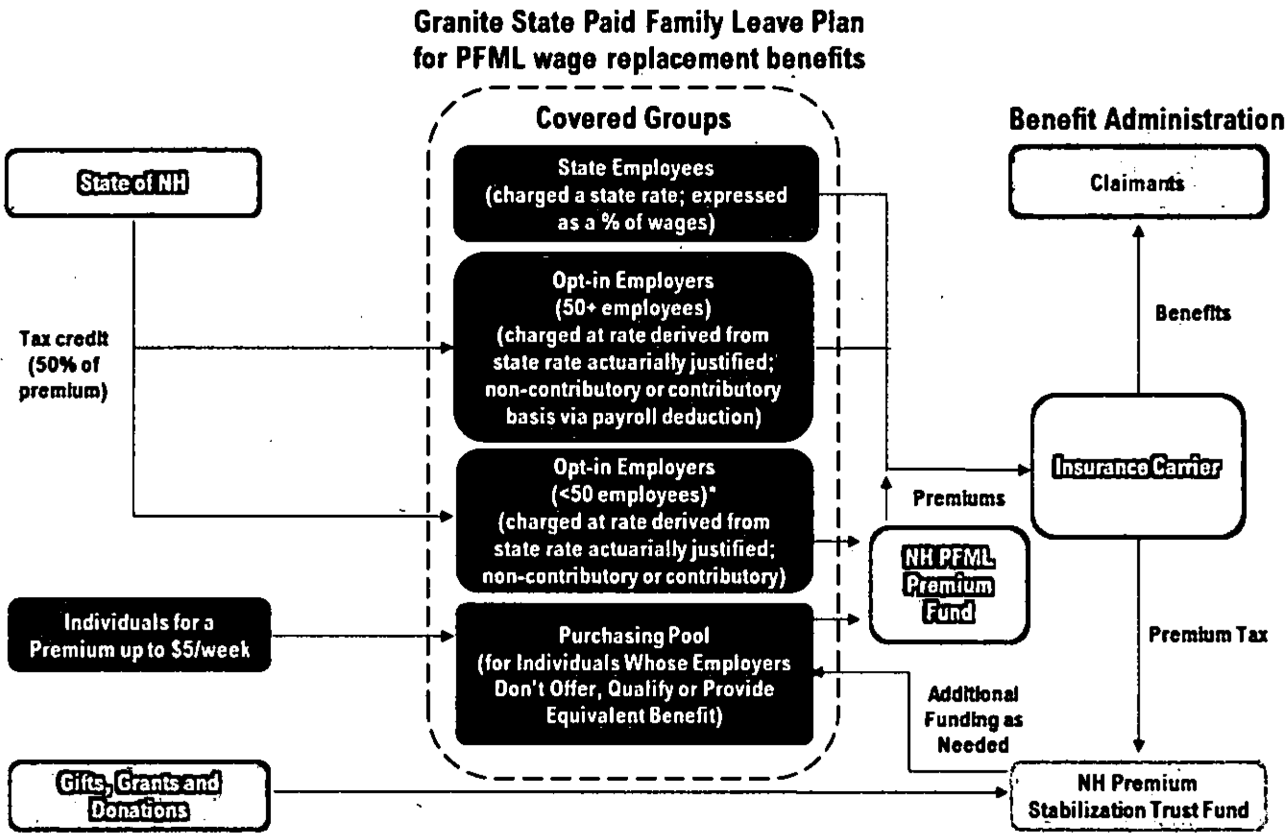
24. ENTIRE AGREEMENT.
Delete Provision 24 Entire Agreement in its entirety and replace with the following:
This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof. Please note the Group Contract governs the terms and conditions of the insurance coverage provided. The Group Contract must be consistent with the terms of this agreement and any applicable laws and regulations.

EXHIBIT B SCOPE OF SERVICES

1. INTRODUCTION

1.1. The Contractor shall provide the State of New Hampshire (hereinafter referred to as the "State"), Department of Administrative Services and New Hampshire Employment Security, with Commercial Insurance Carrier Services for the Granite State Paid Family Medical Leave ("PFML") Plan ("the Plan") in accordance with RSA 21-I:96-108 and RSA 282-B:1-10 and any related statutory changes thereto during the term of the Contract.

1.2. As the Plan shall be in place for state government employees and available for purchase by other public and private employers and individuals by January 1, 2023 as required by RSA 21-I, **time is of the essence in the performance of this Contract. The chart below depicts coverage under the Plan.**


Granite State Paid Family Leave Plan
for PFML wage replacement benefits
Covered Groups
Benefit Administration
State of NH
State Employees (charged a state rate; expressed as a % of wages)
Claimants
Benefits
Tax credit (50% of premium)
Opt-in Employers (50+ employees) (charged at rate derived from state rate actuarially justified; non-contributory or contributory basis via payroll deduction)
Insurance Carrier
Premiums
Opt-in Employers (<50 employees)* (charged at rate derived from state rate actuarially justified; non-contributory or contributory)
NH PFML Premium Fund
Individuals for a Premium up to $5/week
Purchasing Pool (for Individuals Whose Employers Don't Offer, Qualify or Provide Equivalent Benefit)
Premium Tax
Additional Funding as Needed
Gifts, Grants and Donations
NH Premium Stabilization Trust Fund

2. TERMINOLOGY

2.1. Birth and bonding aligns with the FMLA to include the birth of a child and to bond with the newborn child within one year of birth; and the placement with the employee of a child for adoption or foster care and to bond with the newly placed child within one year of placement.

2.2. Care for a family member aligns with the FMLA to include care for the employee's spouse, son, daughter, or parent who has a serious health condition, including incapacity due to pregnancy and for prenatal care.

2.3. Child has the same meaning as "son or daughter" under the FMLA (i.e., a biological, adopted, or foster child, a stepchild, a legal ward, or a child of a person standing in loco parentis, who is either under 18 years of age, or who is 18 years of age or older and incapable of self-care because of a mental or physical disability at the time that FMLA leave is to commence).

2.4. Employee means a person performing services for any employer with a physical location in New Hampshire in exchange for wages under any contract of hire written or oral, express or implied.

2.5. Employer means any individual or type of organization located in New Hampshire, which has in its employ one or more individuals performing services for it within the State.

2.6. Equivalent Benefit means at least the same benefit level (60%) and number of weeks (6) of family and medical leave.

2.7. Family member means a child; a parent; or the child's spouse or domestic partner; a biological, adoptive, foster or step grandparent; a spouse or domestic partner.

2.8. Individual Group is comprised of individuals who work for employers who do not offer either PFML coverage under the Plan as authorized by RSA 21-I:96 through RSA 21-I:108 or a PFML benefit that is at least equivalent to such coverage under the Plan, and who voluntarily opt to purchase coverage through the Plan.

2.9. Intermittent/Reduced Schedule recognizes that benefits shall be available in increments of at least four hours on any one day on an intermittent and continuous basis.

2.10. Own Serious Health Condition aligns with the FMLA to cover a serious health condition that makes the employee unable to perform the essential functions of his or her job, including incapacity due to pregnancy and for prenatal medical care. This type of coverage is only available if the employee's employer does not offer short-term disability coverage.

2.11. Parent means a biological, adoptive, foster, or stepparent, or legal guardian as defined in "family member".

2.12. Permanent State Employee means any full-time employee who has completed their 12-month probationary period with any branch of the State government, including any person who has been or will be employed on a temporary basis for a period of not less than six (6) months in a 12-month period.

2.13. Private Employer means any entity located in New Hampshire and which falls outside the definition of State Employer and Public Employer.

2.14. Public Employer means any political subdivision of the State, any quasi-public corporation, the state community college system and the state university system.

2.15. Qualifying Exigency and Military Caregiver aligns with the FMLA to include any qualifying exigency arising out of the fact that the employee's spouse, son, daughter, or parent is a military member on covered active duty or call to covered active duty status or caring for a covered service-member with a serious injury or illness if the eligible employee is the service-member's spouse, child, parent, or next of kin.

2.16. Serious health condition means any illness covered by the FMLA including treatment for addiction as prescribed by a treating clinician, consistent with American Society of Addiction Medicine criteria, as well as treatment for a mental health condition, consistent with American Psychiatric Association criteria.

2.17. Spouse means an individual who is legally married to the employee.

2.18. State Employer means the State of New Hampshire, including the executive, judicial and legislative branches.

2.19. Wages means every form of remuneration for personal services paid to the employee by the employer, including salaries, commissions, tips and bonuses.

3. CONTRACT DOCUMENTS

3.1. This Contract consists of the following documents ("Contract Documents"):

3.1.1. State of New Hampshire Terms and Conditions, General Provisions Form P-37

3.1.2.	EXHIBIT A	Special Provisions
3.1.3.	EXHIBIT B	Scope of Services
3.1.4.	EXHIBIT C	Method of Payment
3.1.5.	EXHIBIT D	RFP 2571-22
3.1.6.	EXHIBIT E	Contractor Proposal submitted in response to RFP 2571-22

3.1.7. Appendix 1 Proposed NHID Family and Medical Leave Insurance (FMLI) Rules (INS 8000)

3.1.8. Appendix 2 Implementation Milestones

3.1.9. Appendix 3 Technical Capabilities

3.2. 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 in EXHIBIT A "Special Provisions,"); (2) EXHIBIT B "Scope of Services," (3) EXHIBIT C "Method of Payment," (4) EXHIBIT D "RFP 2571-22," (5) EXHIBIT E "Contractor Proposal" (6) APPENDIX 1 Proposed NHID Family and Medical Leave Insurance (FMLI) Rules (INS 8000), (7) APPENDIX 2 Implementation Milestones, and (8) APPENDIX 3 Technical Capabilities.

4. TERM OF CONTRACT

4.1. The term of this Contract shall commence upon the approval by the Governor and Executive Council and shall continue through December 31, 2027 unless extended for additional terms.

4.2. The State may solicit bids for the continuation of carrier services for the Plan prior to the expiration of this Contract. Shall a subsequent contract be awarded to a vendor other than the Contractor, the Contractor shall, cooperate with the State in executing those actions necessary to facilitate a smooth, orderly and complete transition to the next vendor including, without limitation on knowledge and records, and other materials. Any product, whether acceptable or unacceptable, developed under this Contract is the sole property of the State of New Hampshire unless stated otherwise in the Contract.

4.3. The Contract may be extended for up to two (2) years under the same terms, conditions, and pricing structure upon the mutual agreement between the Contractor and the State with the approval of the Governor and Executive Council.

4.4. No payments under this Contract shall take place before January 1, 2023.

5. SCOPE OF WORK

5.1. The Contractor shall obtain and maintain throughout the term of this Contract a license with NHID to engage in the business of insurance in the State of New Hampshire under RSA 401:1, III and IV, and be in good standing in the Contractor's state of domicile.

5.2. The Contractor shall also be responsible for ensuring that all subcontractors or agents providing services under this Contract obtain and maintain any and all required licensing under State and Federal law.

5.3. The Contractor shall also require and ensure that all of its employees, subcontractors and agents who provide services under the Contract maintain all licenses and certifications required by state and federal law.

5.4. Contractor, subcontractors, or agents providing services under this Contract shall carry fidelity and surety insurance or bond coverage and errors and omission insurance throughout the term of this Contract.

5.5. **Minimum Requirements**

5.5.1. Scope of Coverage

5.5.1.1. The Contractor shall fully insure and administer the Plan to its three eligible groups: 1) the State Employer Group, 2) the Private and Other Public Employer Group participants who voluntarily choose to sponsor coverage for their employees, and 3) the Individual Group comprised of individuals who work for employers who choose not to offer PFML coverage or fail to meet minimum participation requirements or do not offer a PFML benefit at least equivalent to the Plan in compliance with the provisions of HB2 and its referenced RSAs and all other applicable State and Federal laws and insurance rules. There is no guarantee of participants beyond the State Employer and it is possible that other carriers may compete for Private and Other Public Employer business.

5.5.1.2. The Contractor shall provide the following scope of coverage for each of the three groups:

5.5.1.2.1. Permanent State Employees:

5.5.1.2.1.1. Coverage for the same types of leave as the federal Family and Medical Leave Act (FMLA), specifically birth and bonding, care for a family member, qualifying exigency and military caregiver, <u>excluding</u> coverage for an employee's own serious health condition.

5.5.1.2.1.2. Wage replacement benefit such that:

5.5.1.2.1.2.1. Eligible employees shall receive 60 percent of their average weekly wage;

5.5.1.2.1.2.2. The maximum duration of wage replacement shall be six (6) weeks per year, subject to a 7-calendar day elimination period; and

5.5.1.2.1.2.3. Wages used to determine the 60 percent PFML benefit shall be capped at the amount of the Social Security taxable wage maximum as amended from time to time.

5.5.1.2.1.3. State employees shall use all accrued allowable paid time before PFML pays.

5.5.1.2.1.4. Premium for coverage shall be charged at a per employee premium amount (the "State Rate") expressed as a percentage of covered payroll.

5.5.1.2.2. Private and Other Public Employers:

5.5.1.2.2.1. Coverage for the same types of leave as FMLA, specifically birth and bonding, care for a family member, qualifying exigency and military caregiver, including coverage for an employee's own serious health condition. Coverage for an employee's own serious health condition does not include leave that arises from a work-related injury and for which there is workers' compensation (WC) coverage or leave that is based upon the insured's status as disabled and for which there is Short Term Disability (STD) or Long Term Disability (LTD) coverage.

5.5.1.2.2.2. Minimum wage replacement benefits such that:

5.5.1.2.2.2.1. Eligible employees shall receive at least 60 percent of their average weekly wage.

5.5.1.2.2.2.2. The wage replacement shall be a minimum duration of six (6) weeks, subject to a maximum duration of 12 weeks per year. A waiting period and elimination period may be included, per negotiations with the employer and as permitted by insurance rules.

5.5.1.2.2.2.3. Wages used to determine the 60 percent PFML coverage shall be capped at no lower than the amount of the Social Security taxable wage maximum as amended from time to time.

5.5.1.2.2.3. Contractor shall recognize that:

5.5.1.2.2.3.1. Private and Other Public Employers may voluntarily choose to provide the minimum coverage above at no cost to their employees or on a contributory or partially contributory basis.

5.5.1.2.2.3.2. Private and Other Public Employers may voluntarily choose to customize their coverage to provide more than the minimum, to the extent it is permitted by the law and insurance rules.

5.5.1.2.2.4. MetLife acknowledges that Employers with 50 or more employees voluntarily opting into the Plan:

5.5.1.2.2.4.1. Shall collect and remit premium directly to the Contractor via payroll deduction;

5.5.1.2.2.4.2. Shall restore employees taking leave to the position held prior to such leave or to an equivalent position by the employer consistent with the job restoration provisions of the FMLA or RSA 275:37-d;

5.5.1.2.2.4.3. Shall continue to provide health insurance to employees during the leave however, employees shall remain responsible for any employee-shared costs associated with the health insurance benefits;

5.5.1.2.2.4.4. Shall not discriminate or retaliate against any employee for accessing family or medical leave wage replacement benefits; and may require that paid leave taken under this program be taken concurrently or otherwise coordinated with leave allowed under the terms of a collective bargaining agreement or other established employer policy or FMLA as applicable.

5.5.1.2.2.5. Employers with fewer than 50 employees voluntarily opting into the Plan shall not be required (but are permitted) to use payroll deduction and may remit payment to the Contractor through the PFML Premium Fund.

5.5.1.2.2.6. Premium for coverage shall be charged at a rate consistent with the insurance department rate filing and is derived from the State Rate through the application of rating factors that are actuarially justified.

5.5.1.2.2.7. Coverage shall be provided through direct contracts either through in house staff or through agents, brokers, and/or consultants with each employer and the Contractor.

5.5.1.2.3. Individual Group:

5.5.1.2.3.1. Coverage for the same types of leave as FMLA, specifically birth and bonding, care for a family member, qualifying exigency and military caregiver, including coverage for an employees' own serious health condition. Coverage for an employee's own serious health condition does not include leave that arises from a work-related injury and for which there is WC coverage or leave that is based upon the insured's status as disabled and for which there is STD or LTD coverage.

5.5.1.2.3.2. Wage replacement benefits such that:

5.5.1.2.3.2.1. Eligible employees shall receive 60 percent of their average weekly wage;

5.5.1.2.3.2.2. The maximum duration of wage replacement shall be six (6) weeks per year, subject to a 7-month waiting period, and a 7-calendar day elimination period;

5.5.1.2.3.2.3. Wages used to determine the 60 percent PFML coverage shall be capped at the amount of the Social Security taxable wage maximum as amended from time to time; and

5.5.1.2.3.2.4. Employees shall use all accrued paid time, except for 1 week, before PFML pays.

5.5.1.2.3.3. Coverage for the Individual Group shall include a 60-day annual open enrollment period so that coverage shall be available for purchase by January 1, 2023.

5.5.1.2.3.4. Premium charged Individual Group participants shall be charged at a rate consistent with the insurance department rate filing;

5.5.1.2.3.4.1. Premium not to exceed $5 per subscriber per week;

5.5.1.2.3.4.2. Premium for individuals who work for employers with fewer than 50 employees may be remitted to the PFML Premium Fund;

5.5.1.2.3.4.3. MetLife will provide notice to employers with 50 or more employees that premium contributions for individuals who work for such employers and seek coverage shall be remitted through payroll deduction conducted by the employer.

5.5.1.2.3.5. Coverage through the Individual Group shall be experience rated.

5.5.2. Administration

5.5.2.1. The Contractor shall perform the following aspects of Plan administration:

5.5.2.1.1. Promote the Plan in collaboration with DAS, NHES and the contractor of the outreach and marketing contract;

5.5.2.1.2. Conduct annual open enrollment procedures with the intent of increasing the number of employees in the state with PFML coverage, as follows:

5.5.2.1.2.1. For the Individual Group, within a 60-day period for coverage which becomes available for purchase January 1, 2023, and can run through March 2, 2023, which can be an annual enrollment season, subject to the Plan's approval;

5.5.2.1.2.2. For Private and Other Public Employers in accordance with their typical procedures at any point during the year, so long as open enrollment is available no later than December 1, 2022.

5.5.2.1.3. New hires can join their employer's plan in accordance with their typical procedures. If the new hire has individual coverage, the individual policy shall end upon coverage being available under their new employer plan. Any premiums paid in advance would be pro-rated and refunded.

5.5.2.1.4. Employees leaving an employer's plan who will not be covered under a new employer's plan will have 60 days from their termination date to purchase an Individual policy.

5.5.2.1.5. Enroll new participants in the Plan at the State, Private and Other Public Employer Group and the Individual Group levels and administer the PFML Premium Fund for deposits of insurance premium payments by developing procedures, and providing mechanisms and systems, as required by the State.

5.5.2.1.6. Collect enrollment, eligibility and employee wage data through paper and electronic formats, the latter of which may include file feeds or Application Programing Interface (API's);

5.5.2.1.7. Collect premium:

5.5.2.1.7.1. Directly from the State;

5.5.2.1.7.2. Through payroll deduction for Private and Other Public Employers with greater than 50 employees;

5.5.2.1.7.2.1. On a self-billed or simplified accounting basis;

5.5.2.1.7.3. Through the PFML Premium Fund (which it will administer on behalf of NHES) for the Individual Group and Private and Other Public Employers with fewer than 50 employees that do not choose to make payments through payroll deduction;

5.5.2.1.7.4. Carry out premium calculations, billing and collection of premium from individuals and employers by check, wire (FED or ACH), credit card or EFT; and

5.5.2.1.7.5. Calculate penalties and grace periods on late payments of premium and conduct the termination process for non-payment.

5.5.2.2. Perform claim intake and customer service for all covered groups through a scalable contact center to serve as an efficient entry point to the Plan for State Employees, Private and Other Public Employees and the Individual Group:

5.5.2.2.1. This shall include facilitating telephonic, web-based and paper claim intake, and addressing questions regarding eligibility, documentation, benefit amounts and payments for triaging calls as appropriate;

5.5.2.2.2. This shall include intake and customer service center hours of operation Monday through Friday 8am-11pm Eastern Time.

5.5.2.2.3. This shall include a contact center that shall be able to ensure assistance by properly trained specialists by live person via telephone, regular mail, and email, and shall send system-generated text messages to claimants under circumstances established by Contractor;

5.5.2.2.4. The contact center shall provide confidential multilingual language translation through a language line and be accessible by the visually and hearing impaired through a text telephone device and relay service;

5.5.2.2.5. The Contractor's contact center shall produce State of New Hampshire specific performance analytics, so long as Contractor's contact center call volume (excluding any subcontractors' call centers) reaches fifty (50) or more calls per day through a toll-free telephone number established by Contractor specifically for enrollees in the Granite State Paid Family Medical Leave Plan, and monthly reporting of telephone activity and in accordance with agreed upon performance guarantees.

5.5.2.3. Perform claims processing, base pay determinations and benefit calculations for all covered groups in an efficient and accurate manner and through proven claims management software systems:

5.5.2.3.1. This shall include:

5.5.2.3.1.1. Claims processing hours of operation Monday through Friday 8am-5pm Eastern Time;

5.5.2.3.1.2. Sending acknowledgement packages within one business day or same day if claimant agrees to electronic correspondence;

5.5.2.3.1.3. Sending a letter to the claimant to follow up on missing information within 5 business days of a new claim opening;

5.5.2.3.1.4. Making initial claim decision, calling the claimant to inform them of such and making benefit payments within 14 days of all necessary information received;

5.5.2.3.1.5. If requested by the claimant, federal income tax shall be withheld from payments, where applicable;

5.5.2.3.1.6. Coordinating with any employer sponsored benefits as appropriate;

5.5.2.3.1.7. Processing appeals by calling and sending a letter to the claimant within 10 business days of the receipt of the appeal letter, and making a final determination within 30 days of receiving all materials; and

5.5.2.3.1.8. Handling claim payment adjustments, including overpayment situations, as necessary.

5.5.2.4. Distribute claimant and employer communications for all covered groups related to claims and appeal processes:

5.5.2.4.1. This shall include claim acknowledgement, approval, extension, denial and appeal communications;

5.5.2.4.2. All letters, emails, forms and other statements will be reviewed with the State during implementation with updates discussed for customization in line with State preferences and applicable regulations;

5.5.2.4.3. Communications shall be transmitted through regular mail, email and uploaded to the Plan's web portal.

5.5.2.5. Provide a web-based portal to support the majority of interaction with employees and employers of all covered groups and administrators of the Plan:

5.5.2.5.1. This shall include 24/7/365 accessibility through the State's website;

5.5.2.5.2. The portal shall facilitate new claim submission, uploading of necessary documentation, viewing status of existing claims, viewing correspondence sent about claims, downloading forms, requesting a call back and sending email to claim representative;

5.5.2.5.3. This shall include advance notification on planned system downtime and timely instructions should the website be down unexpectedly.

5.5.2.6. Perform quality assurance through:

5.5.2.6.1. Monitoring of the end-to-end claim process; the performance of the operations team and the overall results of the Plan;

5.5.2.6.2. Daily audits on a randomly selected claim sample;

5.5.2.6.3. Review of relevant audit metrics;

5.5.2.6.4. Regular manager meetings to review audit findings for coaching opportunities, training needs and process improvements; and

5.5.2.6.5. Regular communication to be determined by the State on audit results.

5.5.2.7. Uphold internal compliance controls and collaborate on ongoing product development by;

5.5.2.7.1. Programing claim management systems accordingly;

5.5.2.7.2. Training account and operational teams to reflect compliance controls and different Plan designs for the State, numerous Private and Other Public Employers and the Individual Group.

5.5.2.8. Apply fraud prevention techniques for all covered groups in accordance with industry standards including but not limited to;

5.5.2.8.1. Initial and continuing identity verification;

5.5.2.8.2. System access security protocols;

5.5.2.8.3. Segregation of duties;

5.5.2.8.4. Investigation services and;

5.5.2.8.5. Training.

5.5.2.9. As directed and approved by the State, provide aggregate and detailed quoting, enrollment, premium and claim reporting on a monthly, quarterly and annual basis for overall administration of the Plan:

5.5.2.9.1. This shall include standard reports for quoting, enrollment, premium, and claim reporting agreed to during the implementation process available on a scheduled basis or through self-service portal and ad hoc and/or customized reports developed on an as needed basis and/or set up to run periodically in PDF, Excel and/or PowerPoint formats and in accordance with the Plan's needs that are expected to evolve over time;

5.5.2.9.1.1. For the State as an Employer;

5.5.2.9.1.2. For Private and Other Public Employers;

5.5.2.9.1.3. For the Individual Group; and

5.5.2.9.1.4. For the Plan Overall.

5.5.2.9.2. This shall include the fulfillment of ad hoc/custom data requests within 5 business days , per the available data elements and any additional costs clearly communicated and approved by the State in advance;

5.5.2.9.3. This shall include a renewal package by July 1, 2026 for 2028 and 2029 and a renewal quote by March 31, 2027 with detailed experience to support another 5-year term;

5.5.2.9.4. This shall include data to support the production of an annual summary report on the PFML Plan which shall be made public and delivered to the Governor, the Senate President, and the Speaker of the House of Representatives as well as required for legislative purposes and the advisory board; and

5.5.2.9.5. This shall include attendance at a mid-year Plan performance review and an annual stewardship review at which time the Contractor will summarize activities and performance for the previous year.

5.5.2.10. Deliver and manage to a detailed, task-oriented implementation plan (samples provided as Appendix 2 Implementation Milestones) that positions the Plan to launch open enrollment in time to make coverage available for purchase no later than January 1, 2023.

5.5.2.11. Support DAS and NHES with their quarterly requirement to provide data and other information and to otherwise work with the PFML Advisory Board, State staff or the Legislature as necessary, including attending meetings onsite as requested.

5.5.2.12. Comply with all applicable state and federal laws and rules including insurance laws:

5.5.2.12.1. The Contractor shall file the rates and forms for the PFML contracts with the insurance commissioner no later than two weeks following Governor and Executive Council approval.

5.5.2.13. Comply and adhere to Appendix 1 Proposed NHID Family and Medical Leave Insurance (FMLI) Rules (INS 8000) which is subject to change.

5.5.2.14. Acknowledge that the Contractor shall refer all media requests to the State and assist the State with responses as well as compliance with the State's 'Right to Know' laws codified as RSA 91-A.

5.5.3. Professional Staffing

5.5.3.1. The Contractor shall provide staffing to include at least the following roles, who may be required, on occasion, to testify in person before legislative and administrative bodies, for which the State will provide as much advance notice as possible:

5.5.3.1.1. **Program Manager:** The Contractor shall assign a dedicated Program Manager who will serve as the primary contact for the services outlined in this Contract, be responsible for the day-to-day client relationship and for ensuring the right resources are carrying out the work. The Program Manager shall be well versed in FMLA, disability and/or leave management and be assigned to the Plan and remain assigned for the term of the Contract, unless agreed by the State in writing to modify the assignment.

5.5.3.1.2. **Marketing/Communications Manager:** The Contractor shall assign a designated Marketing/Communications Manager to provide timely and accurate content to populate the State's microsite, the Contractor's portal, and other relevant locations and documents.

5.5.3.1.3. **Product Development Manager:** The Contractor shall assign a designated Product Development Manager to draft public-facing informational and educational content and provide vendor relationship report of Contractor's TPA to support all Plan participants.

5.5.3.1.4. **Account Management Teams:** The Contractor shall assign a National Accounts team for the State as an Employer, Private and Other Public Employers with 5,000 or more employees and the block of business administered by the Contractor's TPA for under 1,000 size Employers and the Individual Group. The team shall include a Senior Account Executive, Client Services Director and Client Services Consultant. The Client Service

Consultant will serve as a single point of contact for all PFML coverage. For Private and Other Public Employers with 1,000 – 4,999 employees, the Contractor shall assign designated resources that will vary based on group size and existing Contractor, broker and consultant relationships.

5.5.3.1.5. **Contact Center Manager Role:** The Contractor shall assign a designated Director of Claims Operations to oversee PFML insurance claim operations, including operational, financial and service-related requirements to ensure the Plan's needs are being met.

5.5.3.1.6. **Implementation Manager Role:** The Contractor shall assign an Implementation Leader who will be responsible for the successful implementation of the State as an Employer's program within a short time frame.

5.5.3.2. The State reserves the right to approve staff as well as request different staff at any time during the term of this contract if service expectations are not met.

6. TECHNICAL ARCHITECTURE

6.1. To effectively insure and administer the Plan for the three participant groups - State Employees, multiple Private and Other Public Employers, and the Individual Group - the Contractor shall utilize a modern technology/software solution(s) for end-to-end management of policies and claims that is multi-tenant and cloud-based in nature. It shall enable the Contractor's staff to log, process, adjudicate and manage all PFML claims and provide customer support. It shall be rules based to accurately support Plan eligibility and claim determinations. It shall use web services to integrate with data sources and be subject to various security levels. It shall offer a web-based portal to support interaction with the Plan, the State, Private and Other Public Employers and the Individual Group. It shall allow for data and information report production and be reinforced by backup/data recovery features and arrangements to transfer files, services and data processing as appropriate.

6.2. The Contractor shall conform to the specific incidence priority levels, response and resolution timeframes for system support as outlined in Appendix 3 Technical Capabilities.

6.2.1. Data Protection

6.2.1.1. Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of information provided as part of the Plan whether provided by the State, Private and Other Public Employer Groups or participating Individuals at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of such information and comply with the following conditions:

6.2.1.2. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and non-public information. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and non-public data of similar kind.

Contractor Initials

Date 6/17/2022

6.2.1.3. All data obtained by the Contractor in the performance of this contract and all Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data.

6.2.1.4. Unless otherwise stipulated, the Contractor shall encrypt all non-public data at rest and in transit. The State shall identify data it deems as non-public data to the Contractor. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.

6.2.1.5. At no time shall any data that is part of the Plan be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

6.2.1.6. The Contractor shall not use any information collected in connection with the service issued from this Contract for any purpose other than fulfilling the service. Notwithstanding the foregoing, the Contractor may use non-individually identifiable information collected in connection with the service issued from this Contract for the purpose of data compilation, statistical analyses and other studies.

6.2.2. Data Location

6.2.2.1. The Contractor shall provide its Services to the State and its end users solely from data centers within the Continental United States. All storage of Plan data shall be restricted to information technology systems within the Continental United States. The Contractor shall not allow its personnel or sub-contractors to store Plan data on personal portable devices, including personal computers, except as specified and allowed by the contract, and then only on devices that are used and kept at its data centers within the Continental United States. The Contractor shall permit its personnel and Contractors to access Plan data remotely only to provide technical support and as specified or required by the contract. The State acknowledges that the Contractor will from time to time provide confidential translation services from outside of the Continental United States. Under no circumstances shall the provision of such translation services include access to systems containing plan data that is required to be housed and remain within the Continental United States.

6.2.2.2. In performing its obligations under this Agreement, Contractor may gain access to Confidential Information of the State. Confidential Information includes any and all information owned or managed by the State of New Hampshire - created, received from or on behalf of any Agency of the State or accessed in the course of performing contracted Services including any information provided by the State, participating employers or participating individuals - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personally Identifiable Information (PII), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and Confidential Information. The Contractor shall not use the Confidential Information developed or obtained during the performance of, or acquired, or developed by reason of the

Agreement, except as directly connected to and necessary for the performance of the Agreement. Contractor shall maintain the confidentiality of and protect from unauthorized use, disclosure, publication, and reproduction (collectively "release"), all Confidential Information.

6.2.2.3. In the event of the unauthorized release of Confidential Information, Contractor shall immediately notify the State's Information Security Officer, and the State may immediately be entitled to pursue any remedy at law and in equity, including, but not limited to, injunctive relief.

6.2.2.4. Subject to applicable federal or State laws and regulations, Confidential Information shall not include information which:

6.2.2.4.1. Shall have otherwise become publicly available other than as a result of disclosure by the receiving Party in breach hereof;

6.2.2.4.2. Was disclosed to the receiving Party on a non-confidential basis from a source other than the disclosing Party, which the receiving Party believes is not prohibited from disclosing such information as a result of an obligation in favor of the disclosing Party;

6.2.2.4.3. Is developed by the receiving Party independently of, or was known by the receiving Party prior to, any disclosure of such information made by the disclosing Party; or

6.2.2.4.4. Is disclosed with the written consent of the disclosing Party.

6.2.2.5. A receiving Party also may disclose the disclosing Party's Confidential Information to the extent required by an order of a court of competent jurisdiction. Any disclosure of the Confidential Information shall require the prior written approval of the State. Contractor shall immediately notify the State if any request, subpoena or other legal process is served upon Contractor regarding the Confidential Information, and Contractor shall cooperate with the State in any effort the State undertakes to contest the request, subpoena or other legal process, at no additional cost to the State.

6.2.3. Contractor Confidential Information

6.2.3.1. Contractor shall clearly identify in writing all information it claims to be confidential or proprietary upon providing such information to the State. For the purposes of complying with its legal obligations, the State is under no obligation to accept the Contractor's designation of material as confidential. Contractor acknowledges that the State is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. In the event the State receives a request for the information identified by Contractor as confidential, the State shall notify Contractor and specify the date the State will be releasing the requested information. At the request of the State, Contractor shall cooperate and assist the State with the collection and review of Contractor's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be Contractor's sole responsibility and at Contractor's sole expense. If Contractor fails to obtain a court order enjoining the disclosure, the State shall release the information on the date specified in the State's notice to Contractor, without any liability to the State.

6.2.3.2. This covenant in paragraph 10 shall survive the termination of this Contract.

6.2.4. Security Incident Or Data Breach

6.2.4.1. The Contractor shall inform the State of any security incident or Data Breach in accordance with State and Federal law.

6.2.4.2. Incident Response:

6.2.4.2.1. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. Discussing security incidents with the State shall be handled on an urgent as-needed basis, as part of the Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

6.2.4.3. Security Incident Reporting Requirements:

6.2.4.3.1. The Contractor shall report a security incident to the State identified contact immediately if there has been a security incident that affects the security of the Plan's data.

6.2.4.4. Breach Reporting Requirements:

6.2.4.4.1. If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Plan data that is subject to applicable data breach notification law, the Contractor shall (1) immediately notify the appropriate State identified contact, and (2) take commercially reasonable measures to promptly address the data breach.

6.2.4.4.2. The Contractor, shall promptly notify the appropriate State identified contact by telephone and email in accordance with the agreed upon security plan or security procedures if there has been a security incident that affects the security of the Plan's data.

6.2.4.4.3. The Contractor shall at a minimum:

6.2.4.4.3.1. Cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach;

6.2.4.4.3.2. Promptly implement necessary remedial measures, if necessary; and

6.2.4.4.3.3. Document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

6.2.4.4.4. In the event of a Data Breach, the Contractor shall bear the costs associated with:

6.2.4.4.4.1. The investigation and resolution of the Data Breach;

6.2.4.4.4.2. Notifications to participating employers, individuals, regulators, or others required by State or federal law;

6.2.4.4.4.3. A credit monitoring service required by State or federal law; and

6.2.4.4.4.4. A website or a toll-free number and call center for affected individuals required by State or federal law.

6.2.4.4.5. The Contractor shall complete all required corrective actions within a reasonable mutually agreeable time frame

7. ADDITIONAL REQUIREMENTS

7.1. The Contractor shall correct defective work or damages to any part of a building or its appurtenances when caused by the Contractor's employees, equipment or supplies. The Contractor shall replace in satisfactory condition all defective work and damages rendered thereby or any other damages incurred. Upon failure of the Contractor to proceed promptly with the necessary corrections, the State may withhold any amount necessary to correct all defective work or damages from payments to the Contractor.

7.2. The Contractor staff shall consist of qualified persons completely familiar with the products and equipment they use. The Contracting Officer may require the Contractor to dismiss from the work such employees as 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.

7.3. The Contractor or their personnel shall not represent themselves as employees or agents of the State.

7.4. While on State property, Contractor employees shall be subject to the control of the State, but under no circumstances shall such persons be deemed to be employees of the State.

7.5. All Contractor personnel shall observe all regulations or special restrictions in effect at the State.

7.6. The Contractor's personnel shall be allowed only in areas where services are being performed. The use of State telephones is prohibited.

8. OBLIGATIONS AND LIABILITY OF THE CONTRACTOR

8.1. The Contractor shall provide all services strictly pursuant to, and in conformity with the terms of this Contract.

8.2. It is the responsibility of the Contractor to maintain New Hampshire Vendor Registration with up to date contact information.

8.3. 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

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

9.1. 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.

10. CONFIDENTIALITY & CRIMINAL RECORD

10.1. The Contractor shall conduct criminal background checks, at its own expense, and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract, who have been convicted of any crime of dishonesty and/or integrity.

EXHIBIT C METHOD OF PAYMENT

1. CONTRACT PRICE

1.1. The Contractor hereby agrees to provide Commercial Insurance Carrier Services for the Granite State Paid Family Medical Leave Plan in complete compliance with the terms and conditions specified in Exhibit B for an amount up to and not to exceed the Price Limitation specified in Form P-37 Block 1.8, from the Effective Date through the Completion Date. The parties recognize that the Price Limitation in respect of State employees is defined according to the premium calculation set forth in Section 2 of this Exhibit C (the "Formula"). The parties also recognize that if the number of State employees grows, it is possible that the Price Limitation in Form P-37 Block 1.8 may not be sufficient to cover the Contractor's billed rate. Upon a mutually agreed projection showing that the Price Limitation would be insufficient to cover the amounts that will likely become due to the Contractor under the Formula, the Parties will in good faith seek an amendment to increase the Price Limitation to cover such additional anticipated amounts, subject to governmental approvals including but not limited to Governor and Executive Council. If, for any reason, this amendment is not approved by the Governor and Executive Council and, as a result, the Contractor receives an amount less than what would otherwise be due under the Formula for a period of 30 days or longer, the Contractor shall have the right to terminate the Agreement. 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 Completion Date as indicated in Form P-37 Block 1.7. The figure set forth in Form P-37 Block 1.8 applies only to the amount of the insurance services Contractor provides to the State and not to other employers or individuals.

1.2. The Contractor acknowledges and agrees that the rates shown below for the State Employer and the Individual Group are guaranteed for each year in the five (5) year period from January 1, 2023, to December 31, 2027. In addition, they cover any start-up and termination costs, as well as costs to administer the PFML Premium Fund covering the Individual Group and Private and Other Public Employers with less than 50 employee lives that use it.

2. PRICING STRUCTURE

2.1. The Plan coverage rate shall be billed as a percentage calculated from participating employees' wages. Please refer to Table 2.1 for rates associated with respective plans.

2.2. The State shall be responsible for payments associated with the State Employer Group only. Private and Other Public Employer Groups as well as Individual Groups are the responsibility of the respective participants.

Table 2.1 Premium Calculation

Group	Premium Calculation
State Employer Group	0.207% of covered payroll up to the social security maximum

Private and Other Public Employer Group	Premium for coverage shall be charged at a rate consistent with the insurance department rate filing and is derived from the State Rate through the application of rating factors that are actuarially justified
Individual Group	Premium charged Individual Group participants shall be charged at a rate consistent with the insurance department rate filing; not to exceed $5 per subscriber per week

2.3. **Individual Group Experience Rating**

2.3.1. Contractor will calculate the Individual Group experience utilizing claims paid through March 31st of the current year, for prior year incurred claims utilizing the below formula:

2.3.1.1. Premium less Incurred Claims less Expenses

2.3.1.2. Expenses include premium taxes and administrative fees capped at 26% of Premium.

2.3.2. If actual experience for the prior calendar year indicates a loss and if the Contractor has determined funds from the PFML Premium Stabilization Fund created pursuant to RSA 282-B:5 (the "Stabilization Fund") are necessary in order to assure the premiums charged to individual participants in the Individual Group remain stable from year to year and do not exceed $5 per subscriber per week the Contractor may request payment from the Stabilization Fund. The State shall promptly grant Contractor's request for prior years' experience payment from the Stabilization Fund if the Contractor satisfies the requirements of RSA 282-B:5 and Section 2.3 of this Agreement. Such approval shall not be unreasonably withheld by the State.

2.3.2.1. Any such request shall be accompanied by detailed experience rated accounting demonstrating such loss.

2.3.2.2. Such request shall be reduced by any cumulative prior year's gain that has not been previously applied to a prior loss.

2.3.2.3. Further, such request shall be limited solely to amounts from the Stabilization Fund to the extent such funds are available.

3. PERFORMANCE GUARANTEES

3.1. The Contractor agrees to the following performance guarantees and dollars at risk associated with the respective categories calculated against the State portfolio of employees covered per calendar year:

Category	Measurement	Implementation through December 31, 2024	January 1, 2025 through December 31, 2027
Call Abandonment	5% or less of inbound contact center calls are abandoned, based on State specific results, so long as Contractor's contact	2%	3%

Category	Measurement	Implementation through December 31, 2024	January 1, 2025 through December 31, 2027
	center call volume (excluding any subcontractors' call centers) reaches fifty (50) or more calls per day through a toll-free telephone number established by Contractor specifically for enrollees in the Granite State Paid Family Medical Leave Plan		
Speed to Answer	80% of contact center calls are answered within 20 seconds, based on State specific results, so long as Contractor's contact center call volume (excluding any subcontractors' call centers) reaches fifty (50) or more calls per day through a toll-free telephone number established by Contractor specifically for enrollees in the Granite State Paid Family Medical Leave Plan	2%	3%
System Uptime for Call Center and Web Portal	99% availability during regular business hours, excluding scheduled maintenance	2%	3%
Policy Issuance	95% of policy forms will be issued within 10 business days from date all required information is received	2%	3%
Claim Determination	98% of initial claim determinations are made within five business days of receipt and sufficient documentation, based on results for claims submitted by State employees	2%	3%
Claim Payment Accuracy	98% of claim dollars are paid accurately, based on results for	2%	3%

Category	Measurement	Implementation through December 31, 2024	January 1, 2025 through December 31, 2027
	claims submitted by State employees		
Report Production	100% of mutually agreed upon reports are delivered within 15 calendar days after the last day of the period. Other reports may require additional time to produce following the last day of the period.	2%	3%
Account Management Staffing	Account team members will remain constant for the first 18 months of the contract period excluding changes due to resignations, terminations, and promotions	2%	3%
Account Management Response Time	Account Manager will return calls from the State within four (4) hours 95% of the time	2%	3%
Implementation Team Staffing	Implementation team members will remain constant for at least the first 12 months of the contract period excluding changes due to resignations, terminations and promotions	2%	Not applicable
Claimant Satisfaction	Carrier will conduct end of claim surveys where 85% of responses average 4 on a 5-point scale, based on book of business results. STD, LTD and FMLA claimants are included in this survey.	2%	3%
Additional PG - Account Management Satisfaction	Account Management - MetLife will receive, from designated customer respondents, an average for the year of at least a 5 rating on a 7-point scale to the question "Overall Satisfaction with	2%	3%

Category	Measurement	Implementation through December 31, 2024	January 1, 2025 through December 31, 2027
	the MetLife Account Team" on the MetLife Account Management Survey, based on State specific results.		

4. INVOICING

4.1. The Contractor shall prepare and send insurance premium invoices applicable to State employees to the Department of Administrative Services according to an invoicing schedule and format agreed to by the State.

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

5. PAYMENT

5.1. Non-premium payment method (ACH). Payments shall be made via ACH. The Contractor shall enroll with the State Treasury for ACH payments: **https://www.nh.gov/treasury/state-vendors/index.htm**

EXHIBIT D RFP #2571-22

RFP #2571-22 is incorporated here within.

EXHIBIT E Contractor Proposal Response

Contract proposal 2571-22 is incorporated here within.

Appendix 1 Proposed NHID Family and Medical Leave Insurance (FMLI) Rules (INS 8000)

PART Ins 8000 MINIMUM STANDARDS FOR FAMILY AND MEDICAL LEAVE WAGE REPLACEMENT COVERAGE

Statutory Authority: RSA 400-A:15, I; RSA 415-A:2 and 3

Ins 8000.01 Applicability and Scope. Ins 8000 shall apply to all individual and group policies and certificates that provide coverage for family and medical leave wage replacement benefits ("FMLI") which are not covered under other rules and are delivered or issued for delivery in this state on and after the initial effective date of this part. Any policy or certificate of annuity or life, health or accident and sickness insurance that provides benefits for family and medical leave wage replacement, by way of amendment, rider or otherwise, shall comply with this Part.

Ins 8000.02 Definitions.

(a) "Adverse benefit determination" means a denial, reduction, termination of, or a failure to provide or make payment, in whole or in part, for a benefit, including any such denial, reduction, termination of, or failure to provide or make payment that is based on a determination of a participant's or claimant's eligibility to participate in a plan and including a denial, reduction, or termination of, or a failure to provide or make payment, in whole or in part, for a benefit, including on appeal.

(b) "Average Weekly Wage" means the total wages earned by an insured over a specified period of time, divided by the number of weeks in that period.

(c) "Base Period" means the period of time specified in a policy or certificate that will be used in the calculation of wage replacement benefits.

(d) "Benefit period" means the number of days covering a 12-month period during which benefits may be paid to the insured and shall be permitted to be stated as calendar, fiscal year, a fixed period beginning on the effective or anniversary date of the policy, or a rolling period measured by looking back from the employee's first day of family or medical leave.

(e) "Benefits waiting period" is the time measured from the effective date of coverage during which no benefits are provided.

(f) "Beneficiary" means the person or persons designated as such in the application.

(g) "Care" means the participation in providing assistance or supervision to a family member for a serious health condition or bonding with a child.

(h) "Conditionally renewable" means that renewal of the policy is based on certain conditions.

(i) "Disability" means that due to injury or sickness, the insured meets the definition of partial disability, residual disability, or total disability; or the insured meets other disability benefit triggers specified in a disability income protection policy or certificate.

(j) "Disability income protection coverage" means a policy or certificate that provides for periodic payments, weekly or monthly, for a specified period during the continuance of disability resulting from either sickness or injury.

(k) "Eligibility waiting period" means the period of time that an employee must be in the employ of an employer or an individual must be a member of a union or a permitted group association before becoming an eligible for coverage under this part.

(l) "Elimination period" means the length of time beginning with the first day of leave for a qualifying event during which no benefits are paid to the insured.

(m) "Family leave" means leave from work for a qualifying serious health condition or event of the insured's family member.

(n) "Family member" means a biological, step, adopted, foster, or legal guardian of a son or daughter; spouse; a biological, step, adoptive, foster or legal guardian parent or other person as defined as a family member in the policy or certificate.

(o) "Group" policies shall only be issued, as defined below:

(1) A policy issued to an employer, or to the trustees of a fund established by an employer, for which the employer or trustees shall be deemed the policyholder, to insure employees of the employer for the benefit of persons other than the employer, subject to the following requirements:

(a) The employees eligible for insurance under the policy shall be all of the employees of the employer, or all of any class or classes thereof determined by conditions pertaining to their employment, regardless of the wages paid such employees. The policy may provide that the term "employees" shall include the employees of one or more subsidiary corporations and the employees, individual proprietors, and partners of one or more affiliated corporations, proprietors, or partnerships if the business of the employer and of such affiliated corporations, proprietors, or partnerships is under common control through stock ownership, contract, or otherwise. The policy may provide that the term "employees" shall include the individual proprietor or partners if the employer is an individual proprietor or a partnership; and

(b) The premium for the policy shall be paid by the policyholder, either from the employer's funds, or from funds contributed by the insured employees, or from both. A policy on which no part of the premium is to be derived from funds contributed by the insured employees shall insure all eligible employees.

(2) A policy issued to a labor union or Taft-Hartley Trust for the benefit of the members of the labor union, which shall be deemed the policyholder, to insure members of such union for the benefit of persons other than the union or any of its officials, representatives, or agents, is subject to the following requirements:

(a) The members eligible for insurance under the policy shall be all of the members of the union, or all of any class or classes thereof determined by conditions pertaining to their employment, or to membership in the union, or both;

(b) The premium for the policy shall be paid by the policyholder, either wholly from the union's funds or from funds contributed by the insured members specifically for the insurance, or from both. A policy on which no part of the premium is to be derived from funds contributed by the insured members specifically for their insurance shall insure all eligible members; and

(3) A policy issued to a professional employer leasing company that is authorized under RSA 277-B:2(V); 277-B:9-11. The premium for the policy shall be paid by the policyholder.

(4) A policy issued to a bona fide professional association which is legally obligated to regulate the professional requirements and licensure of a regulated profession and satisfies all of the following:

(a) has been in existence for more than five years;

(b) was formed for purposes other than providing insurance;

(c) the policy is issued to the association and the insurer or properly licensed third party administrator administers the plan and issues the certificates to the insureds; and

(d) the association does not receive any compensation, fees, royalties or other consideration in connection with the provision of insurance.

(5) A policy issued to a group that is expressly authorized in applicable statutes.

(p) "Intermittent leave" means periods of non-consecutive leave taken within a 12-month benefit period in intervals of not less than 4 hours in one day.

(q) "Medical Leave" means leave from work because of the qualifying serious health condition of the insured.

(r) "Wages" means the amount of income received by the insured through employment.

Ins 8000.03 Minimum Standards for Benefits for All Policies and Certificates.

(a) All policies shall provide wage replacement benefits that pay a minimum of 60% of the insured's average weekly wage for absence from employment for at least the following reasons:

(1) To care for the insured's parent, spouse or child who has a serious health condition;

(2) Bonding with the employee's child during the first twelve months after the child's birth, or the first twelve months after the placement of the child for adoption or foster care with the employee; and

(3) Because of any qualifying exigency arising from foreign deployment with the armed forces, or to care for a service member with a serious injury or illness as permitted under the federal Family and Medical Leave Act, 29 U.S.C. section 2612(a)(1)(e), if the insured is the service member's spouse, child, parent or next of kin.

(b) All policies shall contain a provision on wages which identifies the various income sources or components that are considered wages and those that are not. The provision on wages shall exclude benefits such as formal sick pay plans, individual and group disability income insurance plans and retirement plans.

(c) In the calculation of wage replacement benefits:

(1) Wages just before qualifying leave began shall be permitted to be considered on a periodic basis so long as the periodic basis is consistent with the treatment of other terms referring to an insured's wages used in the policy and used to arrive at certain wage replacement benefit payment amounts for a claim; and

(2) The base period used in determining wage replacement benefits shall be permitted to include wages of an insured which occurred in excess of one year but no more than 2 years just prior to the qualifying leave for which the claim is made. If the base period used is longer than the immediately preceding 12 months, the provision shall include policy language which allows for use of the highest level of wages during a calendar year or consecutive 12-month basis of an insured occurring during the period in excess of one year but no more than 2 years.

(d) All policies shall provide a minimum of 6 weeks of wage replacement benefits during a 12-month benefit period as a result of qualifying leave pursuant to (a)(1-3) above. Policies shall be permitted to provide benefits for additional types of qualifying leave consistent with the Family and Medical Leave Act and for up to a maximum of 12 total combined weeks of wage replacement during a 12-month benefit period.

(e) Benefits shall be available in increments of at least 4 hours on any one day on an intermittent and continuous basis.

(f) A policy shall be permitted to require an insured to utilize employer sponsored paid time off benefits before insurance benefits under the policy or certificate will be paid.

(g) A policy shall be permitted to require an elimination period, subject to the following:

(1) The elimination period shall not be longer than 7 calendar days;

(2) The insured's intermittent leave for a qualifying reason, consisting of at least 4 hours on any one day, shall count toward satisfying an elimination period; and

(3) The policy or certificate shall not require more than one elimination period per benefit period or specify a separate elimination period for injury and a separate elimination period for sickness. Nor shall the policy be permitted to provide for a separate elimination period for medical leave and a separate elimination period for family leave.

(h) A policy shall be permitted to contain a benefit waiting period of up to 7 months before coverage provides benefits.

(i) A policy or certificate shall be permitted to reserve a subrogation right for payment of wage replacement benefits where the insured receives a payment for lost income from a third party because an act or omission of the third party caused the serious health condition for which leave was taken.

(j) "Non-cancellable" or "non-cancellable and guaranteed renewable" shall be used only in a policy that the insured has the right to continue in force by the timely payment of premiums set forth in the policy until the individual's eligibility for Social Security normal retirement age, during which period the insurer has no right to make unilaterally any change in any provision of the policy while the policy is in force.

(k) Termination of the policy or certificate shall be without prejudice to a loss that commenced while the policy or certificate was in force. The loss of the insured shall be a condition for the extension of benefits beyond the period the policy was in force, limited to the earlier of either the duration of the benefit period, if any, or payment of the maximum benefits.

Ins 8000.04 Required Policy Provisions.

(a) Every policy or certificate shall contain a provision for the payment of any benefits due to an insured that are unpaid at the time of the insured's death shall be payable to the beneficiary designated, or if none are designated, to the estate of the individual. The provision shall state that the insured has the right to change the beneficiary and the consent of the beneficiary shall not be required to terminate or assign the policy, change the beneficiary, or make any other changes in the policy.
(b) Every policy or certificate shall contain a severability provision and a clause instructing that the policy or certificate shall be interpreted or applied so as to avoid a conflict with federal and state law.

(c) The policy or certificate shall provide for payment of benefits to insureds weekly, biweekly, or at such intervals as the employee is customarily paid wages.

(d) The policy or certificate shall provide notice of the insured's right to commence legal action relating to coverage or other contractual disputes.

(e) Each policy of individual insurance or group insurance shall include a renewal, continuation, or nonrenewal provision. The language or specification of the provision shall be consistent with the type of contract to be issued. The provision shall be appropriately captioned, shall appear on the first page of the policy, and shall clearly state the duration, where limited, of renewability and the duration of the term of coverage for which the policy is issued and for which it may be renewed.

(f) Declination of renewal or termination of group insurance provisions shall be as follows:

a. No insurer shall decline to renew a group policy unless the cause of its action is based on one or more of the reasons for declination of renewal stated in the policy;

b. Any reason to decline renewal shall be stated in a group policy and shall be objective in nature;

c. Declination of renewal shall be defined so as to include any termination of a group policy by the insurer for any reason except for nonpayment of premiums; and

d. Notice of nonrenewal or termination of a group policy by the insurer shall provide for at least 45 days prior notice to the policyholder.

Ins 8000.05 Prohibited Policy Provisions.

(a) No policy shall contain a provision that the leave period shall be considered to commence with the date on which written notice is actually received by the insurer.

(b) A policy shall not limit, reduce or exclude coverage by type of sickness, accident, treatment, or medical condition, except as follows:

(1) A serious health condition arising out of:

a. Aviation, except as a fare-paying passenger;

b. Professional sports;

c. Incarceration;

d. Commission of a felony, riot or driving under the influence of drugs, alcohol or combination thereof; and

e. Harm to a family member brought about by the willful intention of the insured.

(c) Arbitration shall be prohibited, except for policies issued pursuant to a collective bargaining agreement that requires arbitration.

(d) Coverage and benefits shall not be reduced or denied on the basis that the insured's employment was terminated as a result of taking leave for a qualifying event for which benefits were sought or where the insured's employer subsequently becomes insolvent, bankrupt or ceases operations.

(e) No policy or certificate shall provide benefits for medical leave that arises from a work- related illness or injury and for which worker's compensation insurance benefits are paid.

(f) No policy or certificate shall provide benefits for medical leave that arises from the insured's disability and for which the insured receives disability income insurance benefits.

(g) Benefits shall not be integrated with or offset by unemployment benefits received by an insured pursuant to RSA 282-A:14.
(h) No policy or certificate shall include provisions for job or employment protections.

Ins 8000.06 Required Claim Provisions.

(a) Health carriers that offer FMLI shall establish and maintain reasonable procedures governing the filing of benefit claims, notification of benefit determinations, and appeal of adverse benefit determinations, hereinafter collectively referred to as claims procedures.

(b) Individual policies and group certificates shall include a description of the process for appealing and resolving adverse benefit determinations which comply with Ins 1001. If applicable to the employer plan sponsor, the process shall comply with the applicable claims procedures under Employee Retirement Income Security Act of 1974, 29 U.S.C., section 1001 and not exempted under section 4 (b) of this Act 29 U.S.C. Section 1003.

(c) The carrier shall provide a claimant with written or, if requested by the claimant, electronic notification of any adverse benefit determination. The notification shall set forth, in a manner calculated to be understood by the claimant:

(1) The specific reason or reasons for the adverse determination;

(2) Reference to the specific policy provisions on which the determination is based;

(3) A description of any additional material or information necessary for the claimant to perfect the claim and an explanation of why such material or information is necessary;

(4) A description of the carrier's review procedures and the time limits applicable to such procedures, including a statement of the claimant's right to bring a civil action following an adverse benefit determination on review.

Ins 8000.07 Required Disclosure Provisions. The following disclosures shall be conspicuously placed on the front page of the policy and certificate:

(a) A statement whether the policy is conditionally renewable, guaranteed renewable, or non-cancellable;

(b) For policies or certificates that do not provide medical leave benefits, a statement in bold indicating the limitation;

(c) A statement as to any benefit limits or reductions due to attainment of certain ages; and

(d) "An employer's granting of leave under the Family and Medical Leave Act or other types of allowable leave does not guarantee benefits under this [policy][certificate]. Granting of benefits for qualifying leave under this [policy][certificate] does not guarantee any right to continued employment or job protection."
Ins 8000.08 Outline of Coverage. An outline of coverage, in the form prescribed below, shall be issued in connection with policies meeting the standards of Ins 8000. The items included in the outline of coverage shall appear in the sequence prescribed:

[COMPANY NAME]

FAMILY [AND MEDICAL] LEAVE WAGE REPLACEMENT COVERAGE

OUTLINE OF COVERAGE

(1) Read Your Policy Carefully—This outline of coverage provides a very brief description of the important features of your policy. This is not the insurance contract and only the actual policy provisions will control. The policy itself sets forth in detail the rights and obligations of both you and your insurance company. It is, therefore, important that you READ YOUR POLICY CAREFULLY!

(2) Family and Medical Leave insurance coverage is designed to provide, to persons insured, wage replacement benefits resulting from a covered serious medical condition or qualifying event under the

Family and Medical Leave Act, subject to any limitations set forth in the policy. Coverage is not provided for basic hospital, basic medical-surgical, or major medical expenses.

(3) [A brief specific description of the benefits contained in this policy.]

(4) [A description of any policy provisions that exclude, eliminate, restrict, reduce, limit, delay, or in any other manner operate to qualify payment of the benefits described in paragraph (3) above.]

(5) [A description of policy provisions respecting renewability or continuation of coverage, including age restrictions or any reservation of right to change premiums.]
Ins 8000.09 Rates. Rates associated with FMLI coverage shall be reviewed and approved in accordance with NHCAR Part INS 4100 or as otherwise indicated under applicable New Hampshire law.

Ins 8000.10 Waiver of Rules.

(a) The commissioner, upon the commissioner's own initiative or upon request by an insurer, shall waive any requirement of this part if such waiver does not contradict the objective or intent of the rule and:
(1) Applying the rule provision would cause confusion or would be misleading to consumers;

(2) The rule provision is in whole or in part inapplicable to the given circumstances;

(3) There are specific circumstances unique to the situation such that strict compliance with the rule would be onerous without promoting the objective or intent of the rule provision; or

(4) Any other similar extenuating circumstances exist such that application of an alternative standard or procedure better promotes the objective or intent of the rule provision.
(b) No requirement prescribed by statute shall be waived unless expressly authorized by law.
(c) Any person or entity seeking a waiver shall make a request in writing.
(d) A request for a waiver shall specify the basis for the waiver and proposed alternative, if any.

Rule Specific State Statute the Rule Implements

Ins 8000.01 – App & Scope RSA 400-A:15, I; RSA 415-A:2 and 3
Ins 8000.02 – Definitions RSA 400-A:15, I; RSA 415-A:2 and 3
Ins 8000.03 – Min. Standards RSA 400-A:15, I; RSA 415-A:2 and 3
Ins 8000.04 – Req. Pol. Prov. RSA 400-A:15, I; RSA 415-A:2 and 3

Ins 8000.05 – Prohibited Prov. RSA 400-A:15, I; RSA 415-A:2 and 3
Ins 8000.06– Req. Claim Prov. RSA 400-A:15, I; RSA 415-A:4-a and 415-A:4-b; 29 CFR 2560
Ins 8000.07 – Req. Disclosures RSA 400-A:15, I
Ins 8000.08 – Outline RSA 400-A:15, I; RSA 415-A:4
Ins 8000.09 – Rates RSA 400-A:15, I
Ins 8000.10 – Waiver RSA 400-A:15, I; RSA 541-A:22, IV

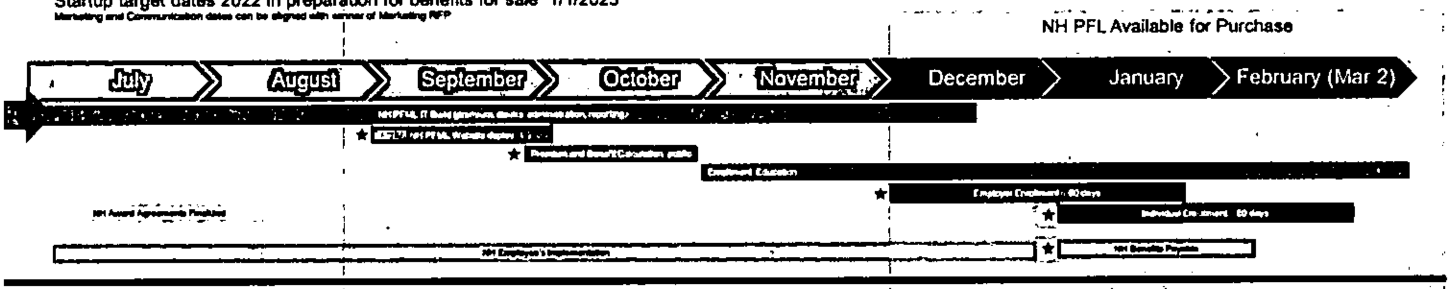
Appendix 2 Implementation Milestones

NH PFML Implementation Milestones

Startup target dates 2022 in preparation for benefits for sale 1/1/2023

Marketing and Communication dates can be aligned with winner of Marketing RFP

MetLife Selected as Preferred Carrier



- Implementation Kick off with all Stakeholders
- Policy Forms drafted
- Marketing Award winner kick off to discuss website and communication planning
- Confirm Participation assumptions for staffing models
- NH Employee's Implementation begins

- Product Rules Developed
- Call Center Training
- Marketing Content for website finalized
- Policy Forms approved by NHID
- Finalize State/MetLife Program level Agreements

★ State NH PFML Web

- Downloadable paystub, employer guide, posters
- Premium & Benefit Calculators finalized
- Call Center toll free may go live, depending on Marketing Plan confirmed in July

- Premium and Benefit Calculators go live
- Publish FAQs
- Enrollment Education materials finalized
- Marketing firm may help with informational videos

- Enrollment Education begins
- Website materials refreshed
- Build systems tested
- Claims staff training
- Communications /Presentations for Enrollment Town Halls and Webinars

★ Employer Enrollment begins

- Policy issue and certification issue process to begin (all plans effective 1/1/2023)
- Website materials refreshed
- Enrollment Marketing / communications ramp up

★ Individual Enrollment begins TPA

★ Claims ready- Benefits payable for NH PFL State employers

- Employer enrollment ends
- Enrollment reporting begins

- Annual Enrollment ends
- Website materials refreshed
- Enrollment materials reviewed with lessons learned for the fall 2023 renewal period

MetLife

Contractor Initials QB

Date 6/17/2022

Appendix 3 Technical Capabilities

The following table represents technical capabilities committed by the Contractor. All references to "Bidder" and "Vendor" mean Contractor in this Agreement.

APPLICATION CAPABILITIES				
State Capabilities		**Bidder Response**		
Capability #	**Capabilities Description**	**Bidder Response**	**Delivery Method**	**Explanation (Bidders are encouraged to attach relevant compliance certificates, audits, etc.)**[1]
GENERAL SPECIFICATIONS				
A1.1	**Ability to access data using open standards access protocol (please specify supported versions in the comments field).**	Yes	Standard	Yes. All client access is through browser.
A1.2	**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	Standard	Data is available in commonly use formats.
A1.3	**Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1**	Yes	Standard	The following technologies comprise the application: Xcode 7.3 , Eclipse , swift, java, HTML5,CSS, AngularJS and Javascript.
A1.4	**Add-on or third-party software required for system(s) to operate for the proposed product.**	No	Standard	MyBenefits is an externally-facing web site accessible to the employees of MetLife's group customers. The website provides access to all the products that the group/user is eligible for. MyBenefits provides a secure environment for employees to access their group benefits information online. The site manages user authentication and also provides a framework for Single Sign-On to the various product dashboards that allow a user to perform transactions (such as enrollment, filing a claim, checking a claim, etc.).

[1] System names and/or descriptions may vary for Contractor's subcontractors, but shall not change the requirements in this section in any material.degree.

				MetLink is a secure, externally facing web site accessible to benefit administrators and brokers of MetLife's group customers. The portal provides users with a variety of capabilities and features that grant access to participant information and enables administrators to conduct transactions supporting the administration of the MetLife products offered.
A1.5	**Dependency on solution(s) not included in this proposal.**	Yes	Standard	There is no dependency on solutions not included in this proposal.
A1.6	**Proprietary components of the software that will be used for the proposed product, such as middleware.**	Yes	Standard	The eBusiness websites sites are proprietary systems and do not require licensing.
A1.7	**Use of Open Source software by the proposed product and degree to which it meets the requirements of RSA chapter 21-R:10, 21-R:11, 21-R:13. http://www.gencourt.state.nh.us/rsa/html/I/21-r/21-r-mrg.htm**	Yes	Standard	Yes. Open Source Software is used many various ways (e.g. Apache, etc.).
APPLICATION SECURITY				
A2.1	**System security in compliance with NIST SP 800-171, Protecting Controlled, Unclassified Information in Non-Federal Systems and Organizations.**	Yes	Standard	Our policies and standards are based on a number of frameworks including NIST. Various IT Risk functions and IT Audits assess compliance to the policies and standards, which in turn provides some alignment to NIST compliance.
A2.2	**System security in compliance with NIST SP 800-63, Digital Identity Guidelines Federal Systems and Organizations.**	Yes	Standard	Our policies and standards are based on a number of frameworks including NIST. Various IT Risk functions and IT Audits assess compliance to the policies and standards, which in turn provides some alignment to NIST compliance.
A2.3	**System security in compliance with NIST SP 800-115, Technical Guide to Security Testing and Assessment.**	Yes	Standard	Our policies and standards are based on a number of frameworks including NIST. Various IT Risk functions and IT Audits assess compliance to the policies and standards, which in turn provides

				some alignment to NIST compliance.
A2.4	**Methods used to ensure that the parties to interactions with the Application cannot later repudiate or rebut those interactions.**	Yes	Standard	Time stamping and digital signatures.
A2.5	**Intrusion Detection methods used to ensure the detection, recording and review of attempted access or modification by unauthorized individuals.**	Yes	Standard	The MetLife network is monitored 24x7x365. Network intrusion detection systems (IDS) are placed around the internet perimeter to monitor for known type of attacks against the MetLife network. The IDS monitors are staggered so that if one IDS system fails to pick up an attack there is a second engine behind the firewall that will catch it. The engines allow MetLife to monitor for attacks both coming into and leaving MetLife.
A2.6	**Privacy methods used to ensure that confidential Data and sensitive communications are kept private.**	Yes	Standard	Yes, there is an internal Privacy Policy which provides guidance on complying with legislative, regulatory and contractual requirements regarding personal information. In addition, external Customer privacy policies can be viewed at: https://www.metlife.com/about/privacy-policy/online-privacy-policy/index.html
A2.7	**System maintenance methods used to ensure that system maintenance does not unintentionally disrupt the security mechanisms of the Application or supporting hardware.**	Yes	Standard	Equipment Maintenance establishes the requirement for regular maintenance. Preventive maintenance shall be performed regularly on all equipment used to support information systems or data center operations in conformance with manufacturer recommendations. This includes hardware for IT platforms (servers, disk arrays, cabling, etc.) and data center environmental and security equipment (fire suppression, environmental controls, etc.) All maintenance tools (e.g. diagnostic and test equipment) carried into a facility by maintenance personnel shall be inspected for obvious improper modifications.

A2.8	**Software patch schedule employed to protect the Software from new security vulnerabilities as they arise.**	Yes	Standard	Security advisory patches are installed based on MetLife's evaluation of the criticality and impact of applying the patches. The following guidelines are followed by MetLife for patches that are designated to be deployed within the environment: Security patches relevant to the protection of sensitive information that have been tested and approved for deployment by Supplier organization will be installed within one month of release.
A2.9	**Ability of 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.**	Yes	Standard	All components have a build document which includes security configuration considerations.

A2.10	**Notification and escalation process in the event of an intrusion.**	Yes	Standard	The MetLife network is monitored 24x7x365. Network intrusion detection systems (IDS) are placed around the internet perimeter to monitor for known type of attacks against the MetLife network. The IDS monitors are staggered so that if one IDS system fails to pick up an attack there is a second engine behind the firewall that will catch it. The engines allow MetLife to monitor for attacks both coming into and leaving MetLife. The IDS systems are managed and monitored by a 24x7 Managed Security Service (MSS). Events are analyzed by the MSS and alerts are generated and sent to the MetLife Incident management and response team for action. MetLife utilizes a three-tiered architecture to protect our data, servers, and internal network. Our DMZ, the demilitarized zone, is the presentation tier. This is where our internet facing servers reside. It provides an area where MetLife can place its content servers for access by our internet customers and creates an area that, if compromised, would limit the exposure to MetLife data. Under normal conditions, traffic is limited from the internet to the DMZ only. Our second tier, known as the bastion, is the application tier. The internet application servers reside in this area and can communicate, on a limited basis, with both the DMZ and our internal network. The third tier, the data tier, resides inside the MetLife internal network. All application and database servers, and application servers and business logic are located in the Bastion behind both sets of firewalls. MetLife uses redundant firewalls in the DMZ and redundant firewalls in the Bastion. In addition to the above, a Data Loss Protection appliance is

					installed at the network perimeter monitoring outgoing traffic for Personally Identifiable Information, a URL filtering proxy filters all outbound browser requests, and email gateway servers check for viruses, malicious attachments, spam and perform content inspection.

A2.11	**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	Standard	MetLife utilizes multi-factor authentication in a number of areas within the Enterprise: • MyBenefits Portal: All web users will receive a validation code via email immediately after a successful login to complete the Device Validation Code (DVC) process, which will register their device and browser combination with MetLife as part of their login process. This includes an additional level of user authentication as part of the login process. The device registration will be applicable for 6 months and the user will be prompted for device registration upon expiration. • Privilege Account: MetLife employs CyberArk to manage privileged accounts. Administrators have to check out an administrative ID in order to perform administrative tasks. Access to CyberArk requires an RSA token for login. Administrators have to check out an administrative ID in order to perform administrative tasks. Users requiring access to the accounts must have an account within CyberArk, access to the vault storing those accounts and a corresponding change ticket for the change. Once accessed, the account activity is logged through CyberArk and the password is automatically changed every 48 hours. • Database: MetLife manages database production access with CyberArk, which authorizes and logs all user activity for the production database. In addition, where contractually

					required for certain customers, MetLife has deployed digital certs to MetLife end points that are needed to access the in scope systems. • Remote access: MetLife requires multi-factor authentication for all individual user access to internal MetLife resources (SharePoint, corporate email, etc.) whenever a user connects to the MetLife network from a network outside of a MetLife office. MetLife employs a combination of hard and soft tokens for an authorized user to access the corporate network from off premises. Coupled with the VPN solution, MetLife uses host-checker software as part of its authentication process to scan each PC to validate that an incoming computer meets minimum security requirements (e.g., running the latest version of malware protection software) before permitting that PC to connect to the MetLife network. • Citrix: As a variation to the multi-factor remote access noted above, MetLife uses Citrix, a virtual desktop control, in combination with a VPN token, to enable third-party consultants to get access to MetLife's systems. The Citrix solution represents a centralized control that manages authorized consultants and contract users connecting to a desktop virtual session. Citrix permits screen updates, mouse clicks, and keystrokes and restricts data being copied or downloaded to a non-corporate device (e.g., MetLife issued laptop). MetLife recently implemented multifactor via RSA token for its

				privileged access management solution,

A2.12	**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	Standard	MetLife utilizes multi-factor authentication in a number of areas within the Enterprise: - MyBenefits Portal: All web users will receive a validation code via email immediately after a successful login to complete the Device Validation Code (DVC) process, which will register their device and browser combination with MetLife as part of their login process. This includes an additional level of user authentication as part of the login process. The device registration will be applicable for 6 months and the user will be prompted for device registration upon expiration. - Privilege Account: MetLife employs CyberArk to manage privileged accounts. Administrators have to check out an administrative ID in order to perform administrative tasks. Access to CyberArk requires an RSA token for login. Administrators have to check out an administrative ID in order to perform administrative tasks. Users requiring access to the accounts must have an account within CyberArk, access to the vault storing those accounts and a corresponding change ticket for the change. Once accessed, the account activity is logged through CyberArk and the password is automatically changed every 48 hours. - Database: MetLife manages database production access with CyberArk, which authorizes and logs all user activity for the production database. In addition, where contractually

				required for certain customers, MetLife has deployed digital certs to MetLife end points that are needed to access the in scope systems. - Remote access: MetLife requires multi-factor authentication for all individual user access to internal MetLife resources (SharePoint, corporate email, etc.) whenever a user connects to the MetLife network from a network outside of a MetLife office. MetLife employs a combination of hard and soft tokens for an authorized user to access the corporate network from off premises. Coupled with the VPN solution, MetLife uses host-checker software as part of its authentication process to scan each PC to validate that an incoming computer meets minimum security requirements (e.g., running the latest version of malware protection software) before permitting that PC to connect to the MetLife network. Citrix: As a variation to the multi-factor remote access noted above, MetLife uses Citrix, a virtual desktop control, in combination with a VPN token, to enable third-party consultants to get access to MetLife's systems. The Citrix solution represents a centralized control that manages authorized consultants and contract users connecting to a desktop virtual session. Citrix permits screen updates, mouse clicks, and keystrokes and restricts data being copied or downloaded to a non-corporate device (e.g., MetLife issued laptop). MetLife recently implemented multifactor via RSA token for its

				privileged access management solution,
A2.13	**Enforce unique user names.**	Yes	Standard	All users of the application have unique identifiers (user IDs).

A2.14	**Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy.**	Yes	Standard	Privileged Password Policy: Privileged accounts are managed via CyberArk and password controls • Privileged passwords will be changed at least every 30 days. • Privileged passwords will be stored and managed in an Enterprise password vault. • Privileged passwords should demonstrate password strength and complexity as followed: • Where possible privileged account password length will be a minimum of 10 characters. • Passwords should use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and special characters. • Passwords should not be serialized (password1, password2, password3). • Passwords should not contain the account name. • No exact word match from a dictionary contained within the password. • Individual privileged account passwords should not be shared. A privileged account may or may not be associated with an individual. If the account is not associated with an individual, it should provide an audit trail pointing back to an authorizing user. These accounts shall be kept to a minimum, individually approved, documented and strictly limited it should provide an audit trail pointing back to an authorizing user. In addition, MetLife utilizes CyberArk to manage privileged accounts. Administrators have to check

				out an administrative ID in order to perform administrative tasks. Users requiring access to the accounts must have an account within CyberArk, access to the vault storing those accounts and a corresponding change ticket for the change. Once accessed, the account activity is logged through CyberArk and the password is automatically changed every 48 hours.
A2.15	**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	Standard	Passwords must be a minimum of eight (8) characters (10 for privileged users) and contain at least two (2) of the following three (3) classes; • Alpha • Numerals (e.g., 0-9) • Non-alphanumeric (special characters) (e.g. ~!@#$%^&*_-+=` | \(){}[]:;'"<>,.?/ MyBenefits: MyBenefits requires 2 of the 3 types below — Must be 8 to 20 characters, at least 1 letter (case sensitive), 1 number and special character allowed: • Alpha • Number

				• Special character Limited to - (dash) and _ (underscore) only
A2.16	**Encrypt passwords in transmission and at rest within the database.**	Yes	Standard	1. Passwords are hashed with an encrypted algorithm. 2. Hashed algorithm is SSHA (Salted Secured Hashed Algorithm). 3. Yes. Unique salts are used along with hashing. 4. SSHA (Salted Secured Hashed Algorithm) is used. The servers are placed in a secure network environment and there are Access Control Instructions (ACI) which protect who has access to different portions of the Directory.

A2.17	**Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy.**	Yes	Standard	Passwords must be a minimum of eight (8) characters (10 for privileged users) and contain at least two (2) of the following three (3 classes; • Alpha • Numerals (e.g., 0-9) • Non-alphanumeric (special characters) (e.g. ~!@#$%^&*_-+=` | \(){}[]:;'"<>,..?/ Passwords cannot be changed by the user more than once in a day Passwords must be changed at least every 90 days (30 days for privileged users, 180 days for external MetLink (60 Days for GSSP MetLink) and not more frequently than once in a 24-hour period. A new password cannot be one of the 12 previously used passwords for a given user ID. Passwords are case sensitive. Company systems will disable a user ID after incorrect passwords are entered no more than six (6) consecutive times for Associates and three (3) consecutive times for MetLink. New User IDs are set to expire at initial log-on. Users should not be allowed to have the following: • A password that is the same as their User ID. • User ID's that consist of all or part of a users' Social Security Number (SSN) or Tax ID Number (TIN)

A2.18	**Provide the ability to limit the number of people that can grant or change authorizations.**	Yes	Standard	The MetLife IT Organization has formally documented Change Control Procedures which ensure that standardized methods and techniques are used for the efficient and prompt handling of all changes in order to prevent change-related incidents. These procedures are used to introduce only approved changes to the production environment without disrupting the availability of systems to MetLife's internal and external customers. All changes to production environments must be quality assured, approved by management, promoted to production in accordance with the Company's production change management procedures and documented in the Company's change-tracking system. Change requests are entered, reviewed and managed in the change control system (ServiceNow). All changes are tested, including unit, QA (stress, performance, functionality testing) and user testing, by the application development teams prior to migrating the change into the general control environment. All changes are reviewed, approved and scheduled by and through the CAB (Change Advisory Board). Changes are reviewed as part of the overall change schedule to avoid collisions. The Change Coordinator must complete the "testing task" within ServiceNow (change tracking software) and

				the change must be approved by the CAB before the change implementation team will migrate the change into production.
A2.19	**Establish ability to enforce session timeouts during periods of inactivity.**	Yes	Standard	User accounts timed out for inactivity varies (from 15 - 30 min) by platform or applications used.
A2.20	**Log all attempted accesses that fail identification, authentication and authorization requirements.**	Yes	Standard	Yes, after 3 failed attempts and until the call center resets their password.
A2.21	**The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.**	Yes	Standard	Logs are captured into a SIEM (Security Information and Event Management) system that manages the logs with capture and archiving rules, and which also has built in rules for identifying and creating alerts related to events associated with the various log sources. The SIEM reports are generated weekly and reviewed by Security Operations. Follow-up on responses from potential violations is done on a case by case basis.

A2.22	**Staff access logs must be kept for (XX- days, weeks, or months).**	Yes	Standard	The MetLife Record Retention Schedule provides the business and legal record retention requirements for the records that you use in performing your job function. The record codes in the record retention schedule are organized by business function (e.g. Accounting, Auditing, Claims, Finance, etc.). Within each business function, there are associated categories of records that relate to the same or similar business process and have similar retention requirements. These have been grouped into enterprise-wide categories referred to as Records Classes. The code, name, description and retention period will be displayed for each record class. The offsite storage of records has been outsourced to Iron Mountain. Iron Mountain provides a system that will enable you to view online your inventory and place your request. There is normally a 24-hour turnaround.
A2.23	**The application Data shall be protected from unauthorized use when at rest.**	Yes	Standard	Encryption of data at rest is implemented at the drive level for SAN, DASD PC Hard Drives and Mobile Devices leveraging AES-256. Mobile phones utilize MobileIron to enforce encryption. Data at rest outside of MetLife (e.g. file transfer) is also encrypted leveraging PGP and AES-256

A2.24	**The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.**	Yes	Standard	MetLife has Data Loss Protection (DLP) infrastructure both at the workstation level and at the network perimeter. DLP agent software, installed enterprise-wide on MetLife DLM (Desktop Lifecycle Management) workstations, monitors for and alerts on confidential data being moved via insecure channels including web uploads, removable devices, email, etc. USB Drives are blocked. The DLP infrastructure at the network perimeter monitors for and alerts on confidential data being moved over the Internet. Both - layered solutions - reduce the risk of inadvertent movement of confidential outside of the MetLife network. MetLife has moved much of their data storage to OneDrive, Teams, and SharePoint sites. Forcepoint is scanning these locations using ForcePoint's Cloud Access Security Broker (CASB), looking for various types of sensitive/confidential information.
A2.25	**Enhancements and new releases planned within the next 24 months.**	Yes	Standard	As part of our broad-reaching solution strategy, we continually invest in the systems, technology and administrative capabilities that support our extensive employee benefit offerings. Our proactive roadmap continually assesses feedback from our customers, their employees, intermediaries and beneficiaries regarding our technology and systems. This feedback helps us decide where to make strategic investments from product innovation and operational enhancement perspectives to update and replace our

				technology allowing us to create the solutions to future issues before they arise.
A2.26	**Required maintenance, security, user input for planned releases.**	Yes	Standard	MYBENEFITS The MyBenefits employee portal is available 24 hours a day, seven days a week, 365 days a year, except for pre-scheduled maintenance windows. The MyBenefits Pre-Scheduled Standard Maintenance Windows are as follows: • Thursday from 9 p.m. to 12 a.m. ET • Friday from 11 p.m. to Saturday 3 a.m. ET • Saturday from 9 a.m. to 12 p.m. ET • Saturday from 9 p.m. to Sunday 12 p.m. ET METLINK The MetLink employer portal is available 24 hours a day, seven days a week, 365 days a year, except for pre-scheduled maintenance windows. The MetLink Pre-Scheduled Standard Maintenance Windows are as follows: • Monday through Friday, between the hours of 11 pm ET and 6 am ET the following morning • Thursday from 9 p.m. to 12 a.m. ET • Saturday from 9 a.m. to 12 p.m. ET • Saturday from 9 p.m. to Sunday 12 p.m. ET

				The maintenance windows above may be extended, as necessary (due to code deployments/upgrades/ website enhancements, etc.), and may prevent the website from being accessed or used during this time period. MyBenefits and MetLink availability as it pertains to performance guarantees is tracked on an ANNUAL basis. Planned activity is typically every week when the site is down for scheduled maintenance which includes regular maintenance, upgrades, fixes, or deployments/releases. To avoid impacting customers, we run maintenance activities after 9 PM ET, and overnight. Website bulletins/messaging is also provided conspicuously on the site that lets our customers know when there may be an impact to website access or functionality during these or other times frames. Unplanned activity, which include unexpected outages or functionality issues, emergency releases, etc., is communicated as soon as it is known/As it occurs to the Account Teams who then communicate this information to their respective customers, including updates regarding issue status and resolution.
A2.27	**Advanced communication of enhancements and releases.**	Yes	Standard	Unplanned activity, which include unexpected outages or functionality issues, emergency releases, etc., is communicated as soon as it is known/As it

				occurs to the Account Teams who then communicate this information to their respective customers, including updates regarding issue status and resolution.
A2.28	**Continued support of enhancement and releases.**	Yes	Standard	Unplanned activity, which include unexpected outages or functionality issues, emergency releases, etc., is communicated as soon as it is known /as it occurs to the Account Teams who then communicate this information to their respective customers, including updates regarding issue status and resolution.
A2.29	**Subsequent application enhancements or upgrades shall not remove or degrade security requirements.**	Yes	Standard	Maintenance activity occurs on a semi-regular basis during established standard weekly maintenance windows. Planned website enhancements (introduction of new feature or functions, etc.) occur throughout the year at different intervals (typically once or twice each quarter), more or less, as needed/planned for.
A2.30	**Utilize change management documentation and procedures.**	Yes	Standard	The MetLife IT Organization has formally documented Change Control Procedures which ensure that standardized methods and techniques are used for the efficient and prompt handling of all changes in order to prevent change-related incidents. These procedures are used to introduce only approved changes to the production environment without disrupting the availability of systems to MetLife's internal and external customers.
TESTING CAPABILITIES				
State Capabilities			**Bidder Response**	

Capability #	Capabilities Description	Bidder Response	Delivery Method	Explanation (Bidders are encouraged to attach relevant compliance certificates, audits, etc.)
APPLICATION SECURITY TESTING				
T1.1	**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	Standard	Per policy, to ensure that information security requirements are treated as an integral part of business requirements, our policy stipulates that security considerations are integrated with design and specification efforts as part of the Security Development Framework (SDF) process.
T1.2	**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	Standard	Systems development and maintenance procedures are initiated, approved and controlled by Programmers and Business Analysts who are responsible for the systems. To ensure that information security requirements are treated as an integral part of business requirements, our policy stipulates that security considerations are integrated with design and specification efforts as part of the Security Development Framework (SDF) process. Our robust quality assurance process tests for both functionality and performance of our applications. Through daily change control meetings, we assess any potential risks, verify back-out procedures, and ensure we have appropriate authorizations for any systems changes.

Contractor Initials QB

Date 6/17/2022

T1.3	**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.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.4	**Test for Access Control; supports the management of permissions for logging onto a computer or network.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting

				issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.5	**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	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf

T1.6	**Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.7	**Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting

				issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.8	**Test the User Management feature; supports the administration of computer, application and network accounts within an organization.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf

T1.9	**Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.10	**Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting

				issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.11	**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	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf

T.1.12	**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	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.13	**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	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting

				issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T1.14	**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.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf

T1.15	**Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
STANDARD TESTING				
T2.1	**The Vendor must test the software and the system using an industry standard and State approved testing methodology.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer

				system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T2.2	**The Vendor must perform application stress testing and tuning.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf

T2.3	**The Vendor must provide documented procedure for how to sync Production with a specific testing environment.**	Yes	Standard	MetLife IT Standards require that application developers include information security features in the application design itself and employ application vulnerability testing throughout the development process. IT Risk and Security (ITRS) provides developers with on-demand services such as the automated vulnerability scanning tool and security knowledge training courses to identify web application security weaknesses and correct them. Vulnerabilities that remain after development are tracked within the Archer system as IT risk findings. Accountability for correcting issues resulting from these reviews resides with individual application development teams. See MetLife Primeon AEH Attestation 8911 MetOnline (Enhanced MyBenefits) for 2021 02182022.pdf and MetLife Primeon AEH Attestation 5089 MetLink Employer Portal for 2021 02182022.pdf
T2.4	**The vendor must define and test disaster recovery procedures.**	Yes	Standard	See Attached MetLife Global Resiliency Overview 01-2022.pdf
HOSTING-CLOUD CAPABILITIES				
State Capabilities		**Bidder Response**		
Capability #	**Capabilities Description**	**Bidder Response**	**Delivery Method**	**Explanation (Bidders are encouraged to attach relevant compliance certificates, audits, etc.)**
OPERATIONS				
H1.1	**Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent.**	Yes	Standard	MetLife has not been Tier rated, but align to industry standard for Tier 4 data centers.
H1.2	**Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage**	Yes	Standard	MetLife maintains two primary data centers within the US. MetLife maintains a data center in Troy, NY and Scranton, PA. The two data centers are active /

	the application and support users with permission based logins.			active meaning that they both have production systems running within the data centers. Designated essential / critical systems will recover at the sister site if one of the locations is impacted by a disaster.
H1.3	**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.**	Yes	Standard	MetLife uses a centralized security management system to control and manage data center access. The access list is reviewed on a quarterly basis. Access can only be approved by the Officer of Data Center Facilities and the Officer of Enterprise Security. Access for employees who leave the company is addressed immediately, through the HR process. Contracted services (e.g. mail room operators) are not given badge access to building. Contactors check in and check out daily at security desk.
H1.4	**Vendor shall install and update all server patches, updates, and other utilities in a timely manner.**	Yes	Standard	Security advisory patches are installed based on MetLife's evaluation of the criticality and impact of applying the patches. The following guidelines are followed by MetLife for patches that are designated to be deployed within the environment: Security patches relevant to the protection of sensitive information that have been tested and approved for deployment by Supplier organization will be installed within one month of release.

Contractor Initials

Date 6/17/2022

H1.5	**Vendor shall monitor System, security, and application logs.**	Yes	Standard	MetLife has several logging infrastructures tailored to the system logging requirements. Production server security logs and firewall logs are captured into a SIEM (Security Information and Event Management) system. This system manages the logs with capture and archiving rules, and which also has built in rules for identifying and creating alerts related to events associated with the various log sources. Production database access is monitored, and events are logged using a database auditing tool. The two systems are fully deployed and integrated into the MetLife Incident Management and response team processes.
H1.6	**Vendor shall manage the sharing of data resources.**	Yes	Standard	MetLife owns its own data centers and does not share the facility or computer systems with other tenants. MetLife leverages logical security controls to segment customer data. This offers an economy of scale that allows for centralized security monitoring and high availability configurations. Customer identifiers at the record level are utilized within the database / application to provide access to MetLife customers.
H1.7	**Vendor shall manage daily backups, off-site data storage, and restore operations.**	Yes	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.

H1.8	**The Vendor shall monitor physical hardware.**	Yes	Standard	The MetLife network is monitored 24x7x365. Network intrusion detection systems (IDS) are placed around the internet perimeter to monitor for known type of attacks against the MetLife network. The IDS monitors are staggered so that if one IDS system fails to pick up an attack there is a second engine behind the firewall that will catch it. The engines allow MetLife to monitor for attacks both coming into and leaving MetLife. The IDS systems are managed and monitored by a 24x7 Managed Security Service (MSS). Events are analyzed by the MSS and alerts are generated and sent to the MetLife Incident management and response team for action. MetLife utilizes a three-tiered architecture to protect our data, servers, and internal network. Our DMZ, the demilitarized zone, is the presentation tier. This is where our internet facing servers reside. It provides an area where MetLife can place its content servers for access by our internet customers and creates an area that, if compromised, would limit the exposure to MetLife data. Under normal conditions, traffic is limited from the internet to the DMZ only. Our second tier, known as the bastion, is the application tier. The internet application servers reside in this area and can communicate, on a limited basis, with both the DMZ and our internal network. The third tier, the data tier, resides inside the MetLife internal

				network. All application and database servers, and application servers and business logic are located in the Bastion behind both sets of firewalls. MetLife uses redundant firewalls in the DMZ and redundant firewalls in the Bastion. In addition to the above, a Data Loss Protection appliance is installed at the network perimeter monitoring outgoing traffic for Personally Identifiable Information, a URL filtering proxy filters all outbound browser requests, and email gateway servers check for viruses, malicious attachments, spam and perform content inspection.
H1.9	**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).**	Yes	Standard	VPN is N/A MetLink is a secure, externally facing web site accessible to benefit administrators and brokers of MetLife's group customers. The portal provides users with a variety of capabilities and features that grant access to participant information and enables administrators to conduct transactions supporting the administration of the MetLife products offered. MyBenefits is an externally-facing web site accessible to the employees of MetLife's group customers. The website

				provides access to all the products that the group/user is eligible for. MyBenefits provides a secure environment for employees to access their group benefits information online. The site manages user authentication and also provides a framework for Single Sign-On to the various product dashboards that allow a user to perform transactions (such as enrollment, filing a claim, checking a claim, etc.).
H1.10	**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	Standard	One key responsibility of the MetLife Privacy Office is the management of data security incidents that may constitute data security breaches. Our process ensures that (i) the right people are alerted, (ii) the breach is appropriately assessed, managed and contained, and (iii) MetLife complies with applicable laws and regulations, identifies lessons learned and prevents future breaches. The MetLife Privacy Office relies on MetLife associates to identify and report potential data security breaches that may occur during the normal course of business. MetLife associates must also report any loss or theft of a laptop computer, discs, tapes or other media, or paper records, containing customer information. MetLife associates must report any such event, regardless of whether the unauthorized access to information occurs at MetLife or occurs at a service provider, such as a third-party administrator, letter shop or

				other vendor that performs business services for us.
DISASTER RECOVERY AND BUSINESS CONTINUITY				
H2.1	**Vendor shall have thoroughly documented disaster recovery and business continuity plans, including architecture and design, that address the recovery of lost State data as well as their own and provide a copy as part of the RFP Exhibit TBD to include items such as the following:**	Yes	Standard	See Attached MetLife Global Resiliency Overview 01-2022.pdf
H2.1a	**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.**	Yes	Standard	See Attached MetLife Global Resiliency Overview 01-2022.pdf
H.2.1b	**Vendor shall adhere to a defined and documented back-up schedule and procedure.**	Yes	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.

H.2.1c	**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	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.
H.2.1d	**Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.**	Yes	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.
H.2.1e	**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	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.
H.2.1f	**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.**	Yes	Standard	MetLife's backup site is a mirror of the production application and infrastructure, and can be activated within 15 minutes (including database and application) in the event of a disaster or critical problem in the production system and therefore is tested continuously.
HOSTING SECURITY				

H3.1	**The Vendor shall employ security measures to ensure that data provided by the State is protected.**	Yes	Standard	MetLife utilizes a three-tiered architecture to protect our data, servers, and internal network. Our DMZ, the demilitarized zone, is the presentation tier. This is where our internet facing servers reside. It provides an area where MetLife can place its content servers for access by our internet customers and creates an area that, if compromised, would limit the exposure to MetLife data. Under normal conditions, traffic is limited from the internet to the DMZ only. Our second tier is the application tier. The internet application servers reside in this area and can communicate, on a limited basis, with both the DMZ and our internal network. The third tier, the data tier, resides inside the MetLife internal network. All application and database servers, and business logic are located in the Application Tier behind both sets of firewalls: MetLife uses redundant firewalls in the DMZ and application tier.
H3.2	**If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.**	Yes	Standard	MetLife has comprehensive encryption standards. Data encryption mechanisms vary based on platform and tools leveraged within the organization. Encryption of data at rest is implemented at the drive level for SAN, DASD PC Hard Drives and Mobile Devices leveraging AES-256. Data at rest outside of MetLife (e.g. file transfer) is also encrypted leveraging PGP and AES-256. TLS is used for MyBenefits and MetLink web access at MetLife. Email encryption is also TLS. TLS v1.2 or TLS v1.3 is used.

H3.3	**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.**	Yes	Standard	MetLife follows industry best practices for the configuration of initial system builds. Servers are built using documented standard procedures and are scanned for compliance. Operating systems are at current and supported operating and application software levels. Compliance scans are run against the production infrastructure on a quarterly basis.
H3.4	**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	Standard	MetLife follows industry best practices for the configuration of initial system builds. Servers are built using documented standard procedures and are scanned for compliance. Operating systems are at current and supported operating and application software levels. Compliance scans are run against the production infrastructure on a quarterly basis.
H3.5	**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	Standard	MetLife has a comprehensive Vulnerability Management Program and Policy that address all identified vulnerabilities and remediates them based upon MetLife's risk ratings. MetLife utilizes various tools such as Qualys, Kenna, Veracode, Jira and RSA Archer to track and manage Vulnerability findings for the organization. Kenna Security, an online vulnerability management tool, measures, monitors, and tracks our overall exposure to threats and vulnerabilities. Kenna Reporting enables MetLife to quickly understand risks, see how we are trending compared to others in the industry, and visualize our ability to reduce risk over time. The Kenna Risk Meter

				brings it all together and contains the results of both MetLife's vulnerability scan data as well as external threat intelligence. The Risk Meter informs us of what risks we incur across all our groups of assets. It summarizes which assets are subject to active Internet breaches, exploits and zero-day threats. The Vulnerability Management Program addresses all identified vulnerabilities and remediate them based upon MetLife's risk ratings and tracks via RSA Archer to close.
H3.6	**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	Standard	The Enterprise Risk Assessment (ERA) program is overseen by Enterprise Risk Management (ERM). MetLife's Board of Directors approved a Risk Management Strategy for adoption in all lines of business. Each business must understand their overall risk appetite, measure each risk with a common framework, and take into account its potential effect on the broader Organization. In addition, MetLife has a comprehensive IT risk management program reporting to ERM. This program is based on repeatable processes that continuously monitor the risk and health of the control environment and related risks through automated tools, assessments, audits and other independent reviews. IT risk management processes represents an enterprise methodology for documenting IT risks, assigning risk ranking, identifying compensating controls and obtaining approval from the business on the

				decisions to accept and/or mitigate risks via action plans. The level of Business Approval is determined based on the residual risk of the IT Risk Finding and the length or presence of a viable Action Plan. Annual risk assessments are performed. Assessments are also performed after system changes that result in the addition of functionality or significant alteration of existing functionality, or when changes in requirements result in the need to process data of a higher sensitivity, or after the occurrence of a serious security violation that raises questions about the validity of an earlier risk assessment.
H3.7	**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	Standard	MetLife has several logging infrastructures tailored to the system logging requirements. Production server security logs and firewall logs are captured into a SIEM (Security Information and Event Management) system. This system manages the logs with capture and archiving rules, and which also has built in rules for identifying and creating alerts related to events associated with the various log sources. Production database access is monitored, and events are logged using a database auditing tool. The two systems are fully deployed and integrated into the MetLife Incident Management and response team processes.
H3.8	**Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.**	Yes	Standard	MetLife follows industry best practices for the configuration of initial system builds. Servers are built using documented standard procedures and are

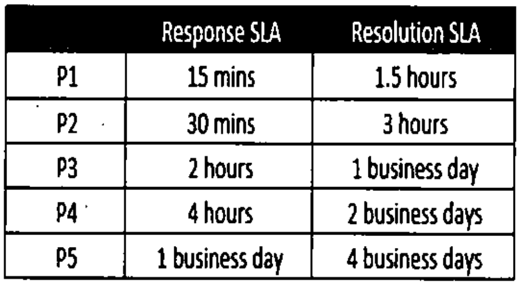
				scanned for compliance. Operating systems are at current and supported operating and application software levels. Compliance scans are run against the production infrastructure on a quarterly basis.
H3.9	**The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.**	Yes	Standard	Whenever notification is legally required to the impacted individuals of a data incident, we offer TransUnion credit monitoring services to those individuals at no cost to them or the employer.
SERVICE LEVEL AGREEMENT				
H4.1	**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	Standard	As long as we have the eligibility file loaded, the goal is always to have MyBenefits and MetLink in production and live on the effective date. Our web portals will be available to for the duration of the contract.
H4.2	**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	Standard	We continually invest in the systems, technology and administrative capabilities that support our extensive employee benefit offerings. Our process continually assesses feedback from our customers, their employees, intermediaries and beneficiaries regarding our technology and systems. This feedback helps us decide where to make strategic investments from product innovation and operational enhancement perspectives.
H4.3	**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	Standard	We continuously invest in the improvement of our claim management systems to improve claim management accuracy, enhance productivity and ensure that we are compliant with all federal, state and local regulatory changes. We also invest in the

				improvement of our Web portal capabilities to bring new self-service options and capabilities to our customers.
H4.4	**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	Standard	Security advisory patches are installed based on MetLife's evaluation of the criticality and impact of applying the patches. The following guidelines are followed by MetLife for patches that are designated to be deployed within the environment: Security patches relevant to the protection of sensitive information that have been tested and approved for deployment by Supplier organization will be installed within one month of release.

H4.5	**The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.**	Yes	Standard	MetLife utilizes a third-party vendor to provide technical support to MyBenefits and MetLink customer users via our technical support help desk, 1-877-9METWEB, which is available Monday through Friday, 8 a.m. to 11 p.m. ET. The help desk is staffed with approx. 60 call center representatives for Tier 1 support and 4 MetLife representatives for Tier 2 support and escalations. Tier 1 supports the following: o Access assistance (including login and registration assistance) o Navigation assistance on all MetLife websites o Unresolved issues are escalated to Tier 2 via referral process o Non-technical product-specific calls are re-routed to the appropriate call center(s) Tier2 supports the following: o Troubleshooting of all errors and issues received through the referral process from the 9MetWeb for MetLife websites o Escalation of unresolved issues For MyBenefits registration/login issues, the user can also be provided with an online pop-up chat session which connects the user with a technical support representative to resolve registration and/or username/password issues. User cannot proactively request a chat session. [Chat is not available via the MetLink website.] The MyBenefits website's 'Help' function also provides product-specific contact information to help

					users resolve issues that may be more product-specific (e.g., Dental or Life claims support, etc.). Customers may also contact their MetLife account representative (Client Service Consultant) directly if they choose to not call the help desk. For MetLink, the current online help function on our employer site, MetLink, provides help for most key fields. While the existing online help is not customized, customized product/feature user guides are available in PDF format online within the site. Static help information is also available via link within the employer (MetLink) and employee (MyBenefits) website. In addition, users may contact our web help desk for assistance at 877-9METWEB.

H4.6	**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	Not Proposing	Our Incident Priority Matrix is outlined below: 1-Critical Major: This is an application, service or infrastructure outage that would affect multiple business functions or sites. There is no workaround available at this time. 2-High Major: This is an application, service or infrastructure outage that would affect multiple business functions or sites with an available workaround. 3-Medium Major: This is an application, service or infrastructure outage that would affect a single business function or site with no available workaround. 4-Low Major: This is an application, service or infrastructure outage that would affect a single business function or site with an available workaround. 5-Best Effort Major: This is an outage impacting an application, service or infrastructure with issues that allow business processing to continue with service degradation.

<table>
<tr><td>H4.7</td><td><b>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.</b></td><td>No</td><td>Not Proposing</td><td>Support issues will be responded to per the guidelines below:
<table><tr><th></th><th>Response SLA</th><th>Resolution SLA</th></tr><tr><td>P1</td><td>15 mins</td><td>1.5 hours</td></tr><tr><td>P2</td><td>30 mins</td><td>3 hours</td></tr><tr><td>P3</td><td>2 hours</td><td>1 business day</td></tr><tr><td>P4</td><td>4 hours</td><td>2 business days</td></tr><tr><td>P5</td><td>1 business day</td><td>4 business days</td></tr></table></td></tr>
<tr><td>H4.8</td><td><b>The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.</b></td><td>Yes</td><td>Standard</td><td>Yes. the MyBenefits employee portal is available 24 hours a day, seven days a week, 365 days a year, except for pre-scheduled maintenance windows. MyBenefits provides real-time data 7 a.m. – 6 p.m. ET Monday – Friday, and 9 a.m. – 4 p.m. ET on Saturday. The MetLink general portal functionality (i.e. Demo; Resources; Forms; Legislative Releases; Profile; etc.) is available 24 hours, seven days a week for customer access.</td></tr>
</table>

H4.9	**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	Standard	Planned activity is typically every week when the site is down for scheduled maintenance which includes regular maintenance, upgrades, fixes, or deployments/releases. To avoid impacting customers, we run maintenance activities after 9 p.m., and overnight. We have bulletins/messaging on the websites that lets our customers know this if they plan to use the websites during these times frames. Unplanned activity, which include unexpected outages or functionality issues, emergency releases, etc., is communicated as soon as it is known/as it occurs to the Account Teams who then communicate this information to their respective customers.
H4.10	**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.**	No	Not proposing	Our performance standard for our websites is 99% availability on an annualized basis. This is included in our proposed performance guarantees.
H4.11	**The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.**	Yes	Standard	The MetLife IT Organization has formally documented Change Control Procedures which ensure that standardized methods and techniques are used for the efficient and prompt handling of all changes in order to prevent change-related incidents. These procedures are used to introduce only approved changes to the production environment without disrupting the availability of systems to MetLife's internal and external customers.

H4.12	**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.**	Yes	Standard	Critical functions are based on the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that are obtained as part of our Business Impact Analysis meetings. Those applications that have little or no tolerance for down time and/or loss data are ranked as being mission-critical systems. As a benchmark, an application that requires either an RTO or RPO of 24 hours or less is considered mission critical.
H4.13	**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	Standard	All changes to production environments must be quality assured, approved by management, promoted to production in accordance with the Company's production change management procedures and documented in the Company's change-tracking system. All changes are tested, including unit, QA (stress, performance, functionality testing) and user testing, by the application development teams prior to migrating the change into the general control environment. The Change Coordinator must complete the "testing task" within ServiceNow (change tracking software) before the change implementation team will migrate the change into production.
H4.14	**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..**	Yes	Standard	The Client Services Team will provide prior notification and applicable training as requested.
H4.15	**The Vendor shall notify the State of any security breaches within two (2) hours of the time**	No	Standard	The Vendor shall notify the State of any security breaches within three (3) business days of the

	that the Vendor learns of their occurrence.			time that the Vendor learns of their occurrence.

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 METROPOLITAN LIFE INSURANCE COMPANY is a New York Profit Corporation registered to transact business in New Hampshire on June 20, 2022. 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: 904542
Certificate Number : 0005794035

SEAL OF THE STATE OF NEW HAMPSHIRE
1776

IN TESTIMONY WHEREOF,
I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 20th day of June A.D. 2022.

David M. Scanlan
Secretary of State

MetLife

METROPOLITAN LIFE INSURANCE COMPANY

ASSISTANT SECRETARY CERTIFICATE

I, Robert Raphael, hereby certify as follows:

1. That I am a duly elected, qualified and acting Assistant Secretary of Metropolitan Life Insurance Company, a New York corporation (the Company).

2. That David S. Brennan is a duly elected and qualified officer and Vice President of the Company, and that this appointment has not been amended, repealed or rescinded and remains in full force and effect as of the date hereof.

3. That the following is a true and correct copy of provisions set forth in Section 5.1 of the By-Laws of the Company:

> "Section 5.1 <u>Instruments</u>. Any officer, or any employee or agent designated for the purpose by the Chief Executive Officer, or a designee of the Chief Executive Officer, shall have power to execute all instruments in writing necessary or desirable for the corporation to execute in the transaction and management of its business and affairs (including, without limitation, contracts and agreements, transfers of bonds, stocks, notes and other securities, proxies, powers of attorney, deeds, leases, releases, satisfactions and instruments entitled to be recorded in any jurisdiction, but excluding, to the extent otherwise provided for in these By-Laws, authorizations for the disposition of the funds of the corporation deposited in its name and policies, contracts, agreements, amendments and endorsements of, for or in connection with insurance or annuities)."

IN WITNESS WHEREOF, I have hereunto set my hand by and on behalf of the Company as of the 8th day of June, 2022.

SEAL
1866

By: ____________________
Name: Robert Raphael
Title: Assistant Secretary

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
06/07/2022

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
Marsh USA, Inc.
1166 Avenue of the Americas
New York, NY 10036
Attn: NewYork.certs@Marsh.com

CN102808112-ALL-4-22-23

INSURED
MetLife, Inc. and its Subsidiaries
200 Park Avenue, 6th Floor
New York, NY 10166

CONTACT NAME:
PHONE (A/C, No, Ext): FAX (A/C, No):
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Old Republic Insurance Company	24147
INSURER B : N/A	N/A
INSURER C : N/A	N/A
INSURER D :	
INSURER E :	
INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** NYC-011335872-01 **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	☒ COMMERCIAL GENERAL LIABILITY			MWZY-312002-22	01/01/2022	01/01/2023	EACH OCCURRENCE	$ 1,000,000
	□ CLAIMS-MADE ☒ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
	☒ CONTRACTUAL LIABILITY						MED EXP (Any one person)	$ 5,000
	□						PERSONAL & ADV INJURY	$ 3,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 15,000,000
	☒ POLICY □ PRO-JECT □ LOC						PRODUCTS - COMP/OP AGG	$ 3,000,000
	□ OTHER:							$
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$
	□ ANY AUTO						BODILY INJURY (Per person)	$
	□ OWNED AUTOS ONLY □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	□ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
	□ □							$
	□ UMBRELLA LIAB □ OCCUR						EACH OCCURRENCE	$
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	$
	□ DED □ RETENTION $							$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY						□ PER STATUTE □ OTH-ER	
	ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N □	N / A					E.L. EACH ACCIDENT	$
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$

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

CERTIFICATE HOLDER

State of New Hampshire
Department of Administrative Services
25 Capitol Street #120
Concord, NH 03301

CANCELLATION

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

Marsh USA Inc.