

# Attachment A

to

RFP No. 4609

Mississippi Department of Employment  
Security (MDES)

## ***Technical Requirements***

ReEmployUSA Application Support,  
Corrective, Adaptive, Preventive, and  
Perfective Maintenance Services

ITS Project No. 45732

# TABLE OF CONTENTS

---

- I. General..... 1**
  - A. How to Respond to this RFP, Attachments, and Appendices..... 1
  - B. Important Attachments and Appendices ..... 2
  - C. A General Overview and Background..... 3
  - D. Procurement Purpose and Goals ..... 3
  
- II. Overview OF THE CURRENT System ..... 6**
  - A. Reemploy USA..... 6
  - B. Overview of Current System - Technical Environment..... 8
  - C. Database..... 9
  - D. Infrastructure ..... 9
  - E. Security ..... 10
  - F. Contact Center and Communications ..... 10
  - G. Microservice Ecosystem..... 11
  - H. Consortium Users – General Information..... 12
  
- III. Vendor Requirements ..... 13**
  - A. Vendor Qualifications ..... 13
  - B. Vendor Capabilities ..... 14
  - C. Staffing Requirements..... 16
  
- IV. Development Practices ..... 21**
  - A. Agile Development Practices..... 21
  - B. Required Product Release Processes ..... 21
  
- V. SOCII Audits ..... 23**
  
- VI. Planning..... 23**
  - A. Enterprise Architecture..... 24
  - B. Development and Quality Management Plan..... 24
  - C. Information Data Security Plan ..... 26
  - D. Transition Plan ..... 29
  - E. Disaster Recovery Plan ..... 30
  
- VII. Definitions..... 30**
  
- VIII. Perfective Maintenance Services / Enhancements ..... 33**

# TABLE OF CONTENTS

---

- A. Perfective Maintenance Service Volume ..... 33
- B. Anticipated Perfective Maintenance Services ..... 34
- C. Perfective Maintenance Service Approval Process..... 34
- D. CORE Perfective Maintenance Service Requirements Processes..... 35
- IX. Maintenance and Support..... 36**
  - A. Maintenance and Support Services ..... 36
  - B. Production Support Services Disaster Recovery: ..... 36
    - i. Security Monitoring..... 36
    - i. Performance Monitoring ..... 37
    - ii. Security Monitoring..... 37
    - iii. Corrective Maintenance Services ..... 38
- X. Administration..... 39**
  - A. Billing Practices ..... 39
  - B. Vendor Capacity..... 41
- XI. Production Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) ..... 42**
  - A. KPI/SLA's ..... 42
  - B. KPI Failure and Maximum Penalties..... 53
  - C. Disaster Recovery SLAs and KPIs ..... 55
  - D. Disaster Recovery KPI Failure and Maximum Penalties ..... 56
  - E. Post-Award SLAs and KPIs ..... 58
  - F. Post-Award KPI Failure and Maximum Penalties..... 59
  - G. Audit and Compliance SLAs and KPIs..... 60
  - H. Audit and Compliance KPI Failure and Maximum Penalties ..... 61
  - I. Corrective Action Plan ..... 62

# Attachment A

## RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

### I. GENERAL

#### A. How to Respond to this RFP, Attachments, and Appendices

1. To properly respond to this RFP, beginning with Item 34 through the end of this document, the Vendor should respond with a written narrative to the requirements listed. Then, the Vendor should respond to *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form* per the instructions in Item 4 below. Finally, the Vendor should note, in *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form*, the appropriate page and paragraph that the Vendor intends as the response to that item. The note must refer to the location of the response in the Vendor’s narrative for that item.
2. This document is created as a reference document to provide sufficient detail for the Vendor to develop its proposal. It works in conjunction with *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form* to RFP Number 4609 entitled *Technical Specifications - Requirements Matrix - Vendor Response Form*.
3. The State shall presume that Vendors have read and agree to all requirements in this RFP. Vendors should take exception to items in which they disagree and may use a separate document to do so. Please reference the document on *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form* listing the page/paragraph of the response.
4. On *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form*, the Vendor must respond with “WILL COMPLY” with an “A”, “EXCEPTION” with an “E”, or “Unable to meet the requirement/service” with an “X” to each point in that document. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide these responses in the Vendor’s narrative and to provide the page and paragraph reference thereto will result in the Vendor receiving a lower score for that item or, at the State’s sole discretion, being subject to disqualification.
5. “WILL COMPLY” (“A”) indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or Vendor’s proposed solution must comply with a specific requirement or must perform a certain task.
6. If the Vendor cannot respond with “WILL COMPLY,” but has an alternative to present, then the Vendor must respond with “EXCEPTION” (“E”). The Vendor must list its alternative solution on the Section V *Proposal Exception Summary Form* and explain the details of its alternative solution in the Vendor Comments column. The Vendor should reference page and paragraph in the Vendor’s response packet. (See Section V of RFP No. 4609 attached and incorporated herein by reference for additional instructions regarding Vendor exceptions.)
7. If the Vendor is not capable of providing the requirement or the service is not available, then The Vendor must list the requirement or service that cannot be provided on the Section V *Proposal Exception Summary Form*. (See Section V of RFP No. 4609 attached and incorporated herein by reference).
8. Where Attachment A asks a question or requests information, the Vendor must respond with the specific answer or information requested in their narrative

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

response and then reference the page and paragraph of that response on the *Attachment B - Technical Specifications Requirements Matrix – Vendor Response Form* Response Form.

9. In addition to the above, Vendors must provide explicit details as to the manner and degree to which their proposal meets or exceeds each specification by responding with the reference to the narrative, including the page and paragraph where the response may be found.
10. In order to accurately and completely respond to this RFP, the Vendor must respond with a currency amount by Consortium State for the following categories as per the instruction in *Attachment C - Cost Information Submission Form*. No additional charges for overhead, travel, or other expenses shall be allowed after Contract award.
  - a. Total for Lifecycle Maintenance and Support by year.
  - b. Total for Lifecycle Travel Costs by year.
  - c. Fully-loaded Hourly Time and Materials Rate.
  - d. Fully-loaded Hourly Perfective Maintenance Service Statement of Work Rate.
  - e. Fully-loaded Hourly Change Order Statement of Work Rate.
11. The specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system. Vendors must specify, in their written Narrative response what additional components may be needed and are proposed in order to complete each configuration.

#### B. Important Attachments and Appendices

12. For the requirements relevant to this procurement, refer to Attachments A, B, C, Appendices A, B, C, D, E, F, G, and H (described below) which are incorporated herein by reference and are considered integral to this RFP. Attachments A, B, C, and Appendices A, B, C, D, E, F, G, and H are posted on the same website location as this RFP No. 4609, and the link is located directly beneath the link for RFP No. 4609. Table 1 lists all appendixes and attachments to this RFP that are attached hereto and incorporated herein by reference.

**Table 1 – List of Appendixes and Attachments**

Title	Name
Attachment A	Technical Requirements – (narrative)
Attachment B	Technical Specifications Requirements Matrix – Vendor Response Form
Attachment C	Cost Information Submission
Appendix A	Consortium Supporting Software and Services
Appendix B	Disaster Recovery Response Plan
Appendix C	Consortium Cloud Resources
Appendix D	Software Development Performance Monitoring
Appendix E	Application System Details
Appendix F	MDES Artificial Intelligence Governance Policy

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

Appendix G	Maine IT Service Contract
Appendix H	Consortium System Overview

#### C. A General Overview and Background

13. The Mississippi Department of Employment Security (MDES) is seeking a Vendor or team of Vendors to provide Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services, for ReEmployMS/USA and to interface and collaborate with the agency's cloud services Vendor for ReEmployMS/USA (hereinafter, "the Project"). The ReEmployMS /USA system is a complex, cloud-hosted Unemployment Insurance solution. For reference purposes, all documents within RFP 4609 the term "Vendor" may be defined as: all vendors, third parties, and/or subcontractors that vendor has assembled for this project.
14. MDES developed and has operated this system for twenty years starting with a solution for Mississippi and, more recently, adding solutions for other states including Maine through the Maine Department of Labor ("MDOL"). MDES and as part of the ReEmployUSA Consortium has a strong desire in furthering its mission of administering and optimizing its various unemployment benefits, job search, and development systems for all Mississippians. In alignment with its mission, MDES envisions improving the security, simplicity, and innovative solutions in its enterprise-wide ReEmployUSA system with more modern and modular functions to better assist with the delivery of the programs for which it is responsible. MDES and Maine seek solutions that focus upon efficiency, effectiveness, and modularity.

#### D. Procurement Purpose and Goals

##### Purpose

15. The purpose of this Request for Proposal (RFP) is for Mississippi and Maine (the "ReEmployUSA Consortium" or "Consortium") to seek a Vendor or team of Vendors who present a technical strategy to maintain, operate, modernize and simplify its Unemployment Insurance (UI) (Benefits, Tax, and Appeals) information technology system; delivers in accordance with that strategy, a comprehensive plan to implement the strategy; and, executes that plan to maintain reliability and implement efficient perfective maintenance services.

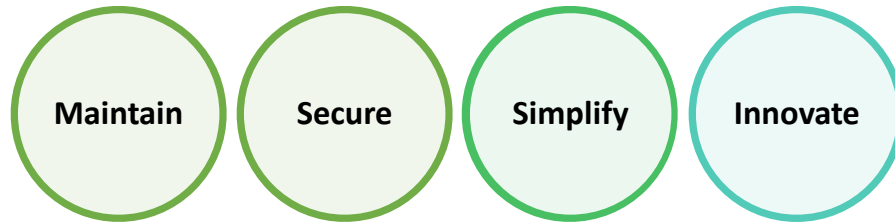
##### Goals

16. The ReEmployUSA Consortium seeks a solution that is simplified, modular, and provides above industry-standard security features. ReEmployUSA Consortium expects the successful Vendor to achieve this goal by updating and modernizing the existing system as well as developing shared solutions (also referred to as "CORE") for all Consortium States with these characteristics. Figure 1 below provides the goals for the ReEmploy Consortium.

## Attachment A

# RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

**Figure 1 - Goals**



17. To achieve these goals, the ReEmployUSA Consortium seeks to:
- i. Modernize existing application code and architecture for ReEmploy.
  - ii. Isolate each Consortium state’s application to eliminate shared dependencies that inhibit innovation. Also, develop an independent build and deployment mechanism for each Consortium State.
  - iii. Collaborate with the Vendor to update the system focusing upon flexibility and a faster process to incorporate statutory and regulatory changes from federal and state government.
  - iv. Improve system resiliency to dramatic fluctuations in demand.
  - v. Increase the use of automation to reduce errors and increase efficiency related to manual tasks as well as reduce batch processing.
  - vi. Improve security by isolating and reducing the access for all remote Vendors and ensure protection of the system from new and emerging threats.
  - vii. Establish robust maintenance and support services to ensure ongoing system performance.
  - viii. Modernize application interfaces and user authentication mechanisms to reduce the backend legacy network connectivity with other systems. Table 2 below provides the priority areas of focus for ReEmployUSA.

**Table 2 - Priority Areas of Focus for ReEmployUSA**

Priority Level	Area of Focus	Description
1	Maintenance and Operation of Existing System	Ensure the continued reliability, stability, and performance of the current system through ongoing maintenance and operational support.
2	Security	Safeguard the system and data from threats and vulnerabilities by implementing robust security measures and practices.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

3	Assessment of Current System and Policies	By working closely with staff and consuming in-depth documentation, the Vendor will need to get quickly up to speed on the current state of the existing system to support a transition to a modern system.
4	Workflow Optimization	Analyze and streamline existing workflows to improve efficiency, reduce redundancies, and enhance overall performance.
5	Design System Enhancements	Work with stakeholders to gather suggestions and requirements for system enhancements.
6	API Integration	Leverage staff knowledge and documentation to draft a data schema to begin building a bridge API. Build an encasement layer to transform data and APIs.
7	Front-End Interface Design and Development	Design and develop a modern front-end interface for specific functions, as identified in collaboration with staff. Employ user-centered design principles and agile development methodologies to ensure the interface delivers quick value to end-users and is data-driven. Explore and implement smaller, strategic user experience improvements for existing interfaces to achieve high-impact, quick wins. After initial design, conduct user testing to gather feedback, refine priorities, and validate new functionalities early in the modernization process.
8	Data Model Development	Create a new data model to support emerging functions and ensure it aligns with the enhanced system requirements
9	Database Querying Capabilities	Implement design features and functions that facilitate easy and efficient querying of the database by the State’s staff to support their operational needs.
10	Support for Modern Software Development Practices	Enhance and support ongoing efforts to modernize software development practices and improve time to delivery by integrating automated testing, Continuous Integration (CI)/Continuous Delivery (CD), Agile methodologies, and user-centered design principles.
11	Performance Optimization	Enhance and support performance optimization techniques.



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

12	Reporting and Data Analysis	Enhance and support the existing reporting database and tools to provide more efficient report generation. Provide advanced data analysis solutions to leverage the data collected to support business decision-making processes.
13	Scalability and Reliability	Enhance the scalability and reliability of the application and ensure that the proposed solutions support future growth and can adapt to changing requirements.
14	Innovation and Futureproofing	Suggest innovative solutions and technologies that can future-proof the system and enhance its capabilities.

## II. OVERVIEW OF THE CURRENT SYSTEM

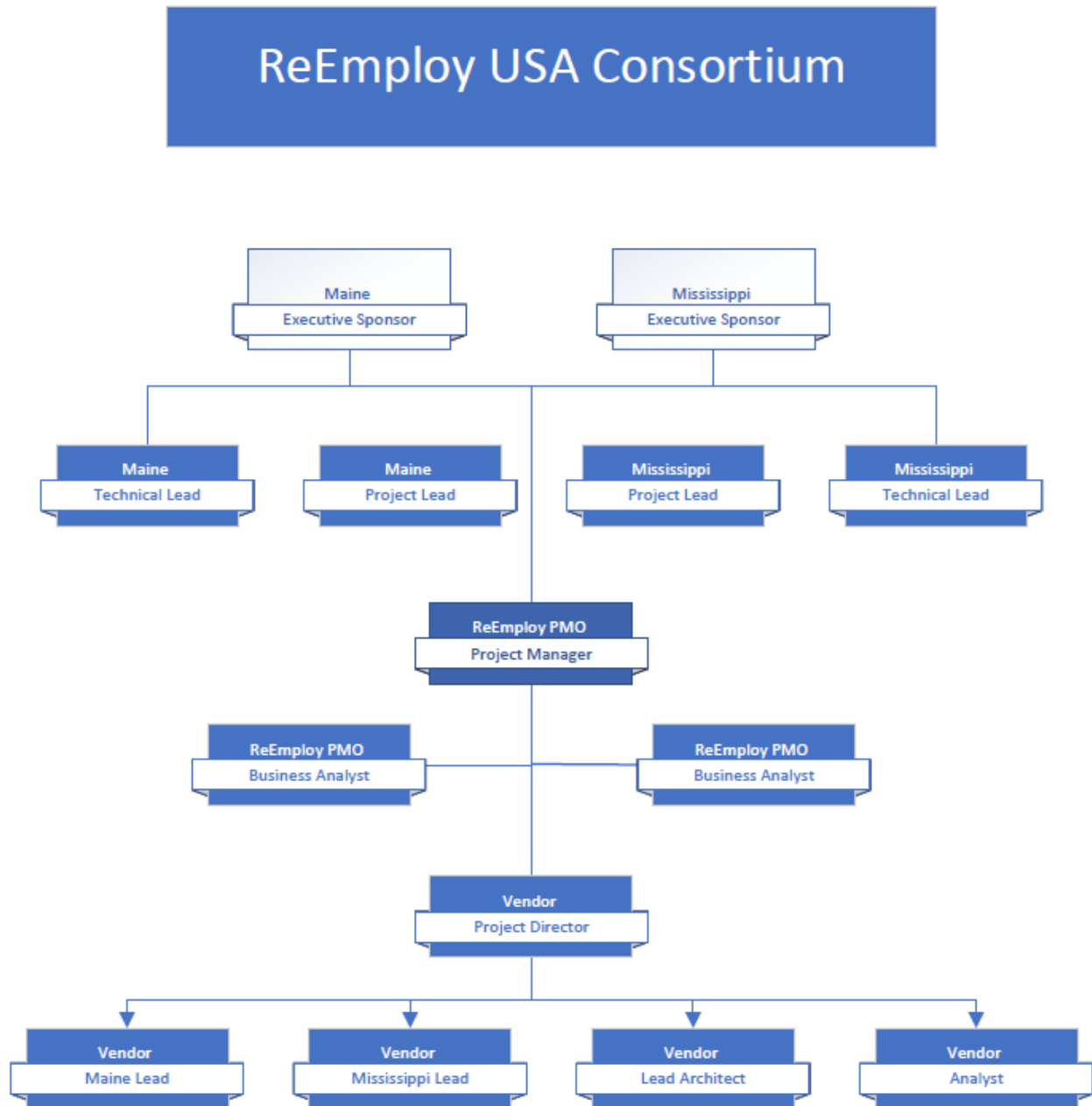
### A. Reemploy USA

18. The ReEmployUSA system has been a highly successful collaboration among multiple states that has led to a stable UI platform. It is also distinguished by reaching the milestone of being the first fully integrated, multi-tenant, cloud hosted UI system. The system has been continuously elaborated since 2004. MDES and the Consortium employ an “always modern” approach to application development to reduce the scope of a system-wide modernization project.
19. MDES and the Consortium share the CORE of the system equally among the group. Each state requires its own instance of the CORE running an individual cloud environment. The Consortium strives to maintain the CORE at approximately 80% of the solution, excluding state specific perfective maintenance services to each of the instances.
20. Figure 2 below shows the MDES and the ReEmployUSA Consortium organization chart, including Consortium and Vendor positions and/or roles and their hierarchical relationships within the project team.

# Attachment A

## RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

Figure 2 – ReEmployUSA State System Organization



21. ReEmployUSA Project Management Officer (PMO):

- i. The ReEmployUSA PMO functions as the liaison between the states and a conduit for the Vendor to MDES or other Consortium states. The PMO is the lead Consortium/MDES resource for monitoring performance, issue resolution and invoicing for the Vendor. The PMO is authorized by MDES and the Consortium States to enforce and implement policies and procedures related to the management of the delivery of products, services, and resources to, and amongst, ReEmployUSA Consortium members.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- ii. The PMO reviews the Vendor's invoices for accuracy. The Vendor will submit invoices to the PMO three (3) days prior to sending the invoice to the states. The Consortium Members may assign a party to perform this review at their discretion.
- iii. The Vendor will work with the PMO to negotiate CORE time and materials and/or fixed price work. The Vendor will also work through the PMO for prioritization on CORE perfective maintenance services.
- iv. The PMO will monitor the performance of the Vendor and work with the Vendor when remediation is required for subpar performance.
- v. The Vendor will ensure with PMO oversight adherence to all policies, procedures, and development standards in the course of its work.
- vi. System performance will be monitored through the metrics outlined in Appendix D - *Software Development Performance Monitoring*. Performance metrics will be compiled by the PMO and provided to the Vendor. The PMO will compile and distribute metrics every 180 days or more frequently if required.
- vii. The Vendor will be required to self-monitor performance. Failure of the PMO to provide reports on any level is not a valid reason for the Vendor to miss targets.
- viii. Failover testing to be conducted no less than every 365 days, either physical or simulated. The testing criteria must be pre-approved by the PMO.
- ix. Failback testing to be conducted no less than every 365 days either physical or simulated. The testing criteria must be pre-approved by the PMO.
- x. The Vendor will communicate all changes to the technical and business roadmaps to the PMO as they occur and provide updates no less than every 180 days. Failure to timely deliver updated technical and business roadmaps to the PMO may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.

#### **B. Overview of Current System - Technical Environment**

- 22. The existing system features a multi-tiered architecture based on Java, with an upgrade to JSF implemented in 2017. It includes a variety of client-facing applications accessible via web browsers, batch applications, interfaces, and interactive response scenarios. The system operates over 2,000 batch processes that are primarily used for reporting and data analysis. Many of these batch processes are automated and time-driven, ensuring timely execution of critical functions. Appendix E - *Application System Details* provides additional information regarding the current system.
- 23. The architecture supports over 350 REST interfaces, which are primarily shared with other state and federal entities, facilitating extensive data sharing and integration. The middle tier of the architecture is designed to simplify application complexity by effectively connecting the browser to the web services, utilizing a lightweight application server to expedite the development lifecycle and minimize the amount of required code. The application is predominantly hosted on Amazon EC2 instances. Table 3 below provides a metric overview of the current system.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

**Table 3 – Metric Overview of Current System**

AREA	METRIC
Application Size	3M lines of CORE, ~600k lines of code specific to each state
Instances	1 Instance per state with a varying number of Virtual Machines by state
Screens	~3,000 screens across Tax, Benefits, Appeals, and Workforce Services
Batch Programs	Over 2000 batch process with 40% being common between the states
IVR Solution	SwampFox and Cisco
Interfaces	~350 SOAP and REST
Operating System	LINUX
Microservices	42

#### C. Database

24. The primary database system is DB2, hosted on Amazon EC2 instances. Prior to the award of the contract, the Consortium States will convert to AWS Aurora. Data is encrypted at rest to ensure security and compliance with regulatory requirements. The database includes numerous controls to protect against internal and external threats. Given the database contains Federal Tax Information (FTI), it is subject to additional security measures as outlined in IRS publication 1075, which exceeds the standard protections for Personally Identifiable Information (PII). Frequent batch jobs are executed to perform various business functions, ensuring data integrity and operational efficiency. A separate reporting database is maintained to support the generation of various reports, enabling detailed analysis and decision making

#### D. Infrastructure

25. Each state manages its own Virtual Private Cloud (VPC) hosted by AWS, ensuring localized control and management of resources. Secure tunnels are established between the core functionality VPC and the state VPCs to ensure secure and reliable communication. This infrastructure setup allows for a flexible and resilient environment that can adapt to the specific needs of each state while maintaining a high level of security and performance. A current list of important information can be found in *Appendix A - Consortium Supporting Software and Services*. Also, *Appendix C - Consortium Cloud Resources* provides a detailed list of the current Consortium Cloud Resources. Table 4 below provides the Metric Overview of Infrastructure.

**Table 4 - Metric Overview of Infrastructure**

Location	VM	CPU	Memory (MB)	Storage (GB)

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

Mississippi	34	126	596	6,844
Maine	30	58	233	3,780
Common	14	34	128	4,426
Totals	78	218	957	15,050

#### E. Security

26. All states utilize common security tools, with the exception of ID proofing and web application firewalls (WAF). One state has implemented a dual-tier WAF strategy, utilizing both Virtual Machine (VM)-based and cloud-based WAFs to enhance protection against Distributed Denial of Service (DDOS) attacks and bot traffic. The other state relies solely on VM-based WAFs for their security. Data encryption is enforced both at rest and in motion, providing a comprehensive approach to data protection. Additionally, each state employs extra encryption measures for FTI data to ensure compliance with federal regulations and to safeguard sensitive information.

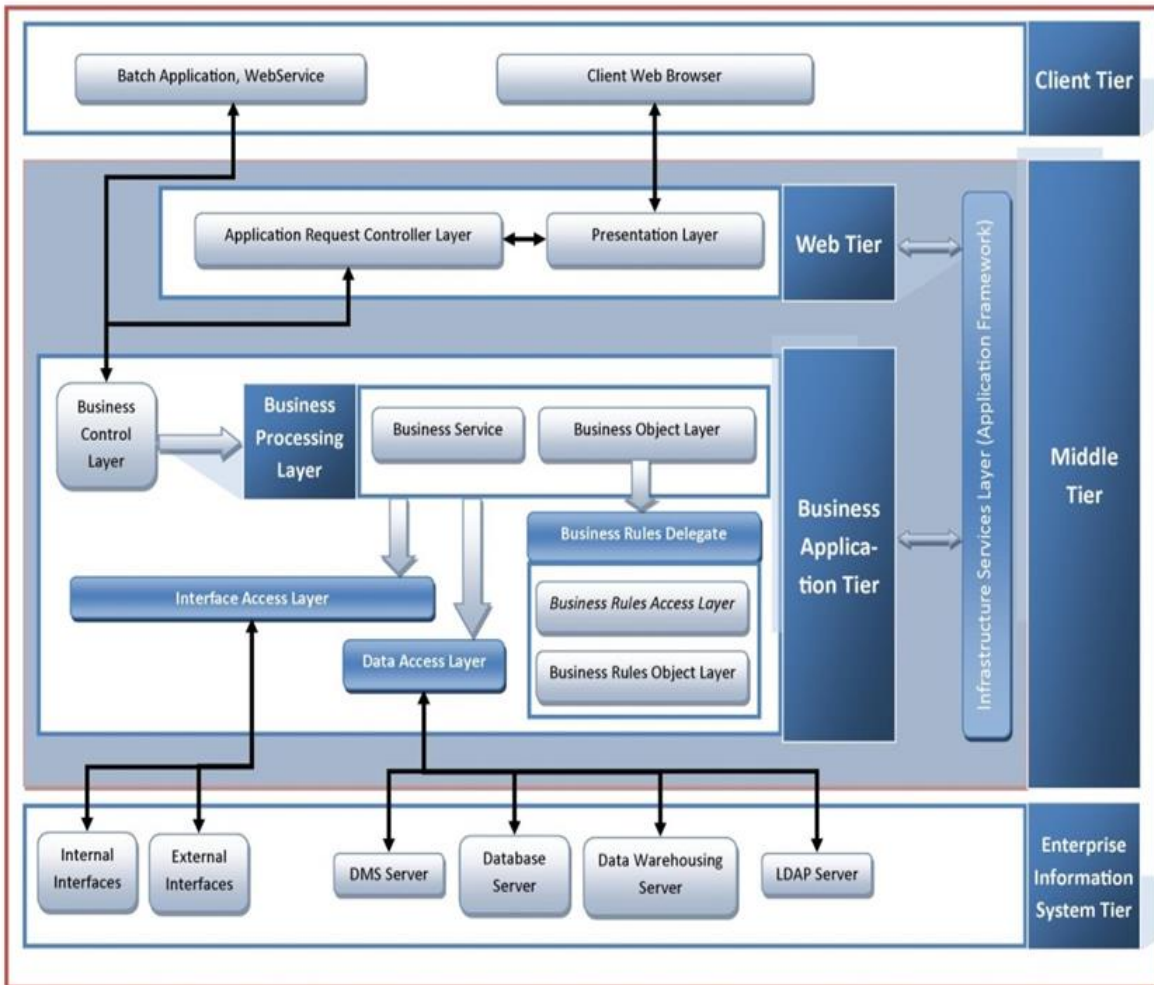
#### F. Contact Center and Communications

27. The Contact Center's base platform of Cisco (Mississippi) and SwampFox (Maine) are not generally considered as part of ReEmployUSA. However, the Consortium states anticipate that perfective maintenance services to the Contact Centers that are supported by ReEmployUSA and integrated with the systems will likely occur within the next five (5) years. Perfective maintenance services may include features like AWS Connect, Avaya ACNS messaging (MDES), and Kore.AI. The Consortium States are using AWS Connect to add capabilities to the Contact Center by adding generative AI features. Kore.AI is used for chatbot functions. Avaya ACNS messaging is used for text messaging to MDES customers. Figure 3 provides an Overview of this Technical Environment. Appendix F - *MDES Artificial Intelligence Governance Policy* explains the permissible and prohibited requirements for use of AI for this agency.

**Figure 3 - Overview of Technical Environment**

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services



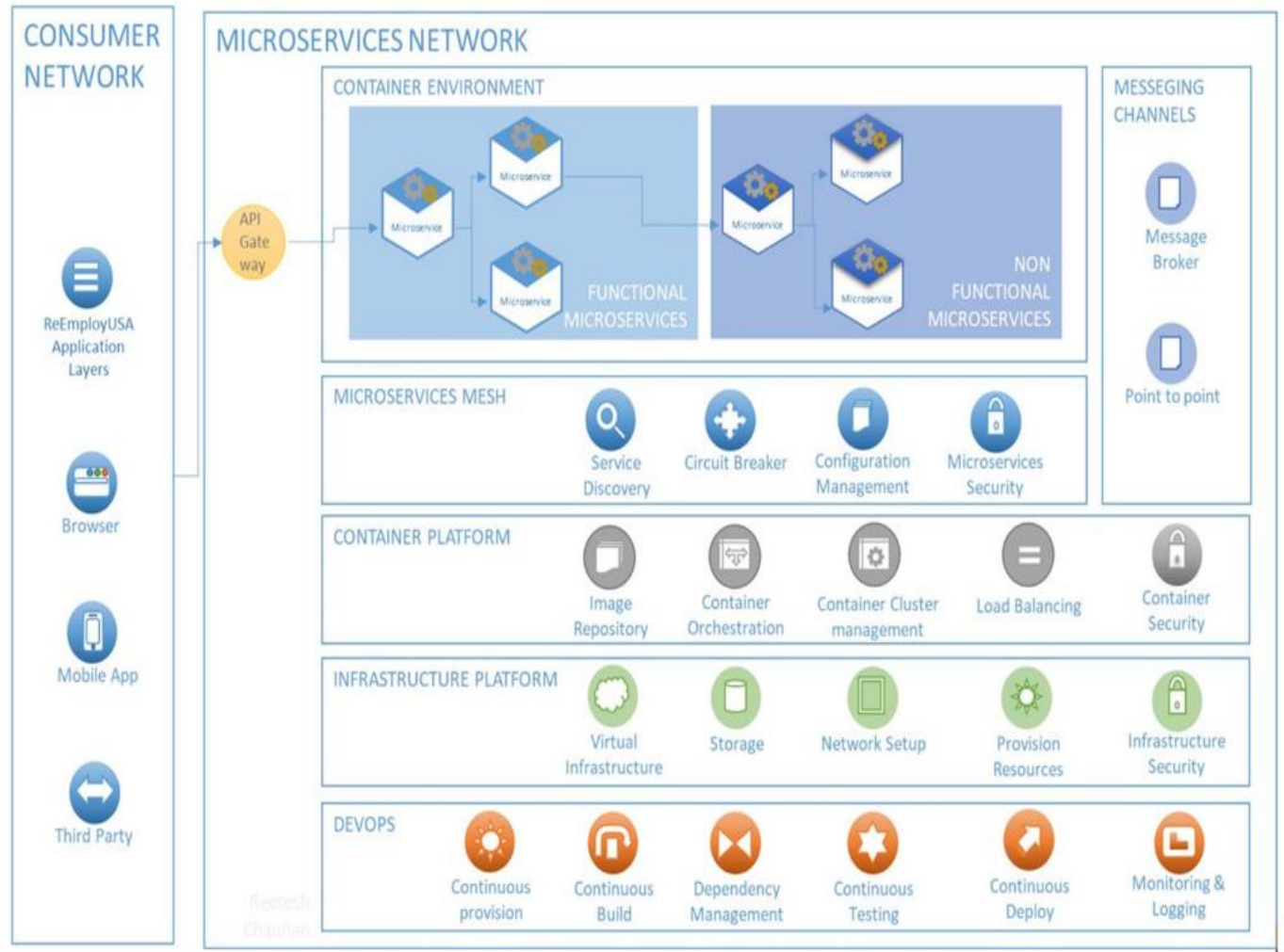
#### G. Microservice Ecosystem

28. The Consortium is moving to a more modular architecture to increase scalability and to make modules easier to share with other states. The current microservice architecture utilizes a common data store. Services are developed using an Angular front end and connected to a Springboot back end. There are 42 microservices created at this time and the largest block will create a new claimant portal experience for UI customers. Figure 4 describes the Microservice Ecosystem.

**Figure 4 - Microservice Ecosystem**

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services



#### H. Consortium Users – General Information

29. Each Consortium state provides its own VPN support. The rules and configuration of VPN services lie with MDES currently.
30. “Core code” is defined as all custom code necessary to operate the ReEmployUSA system and may also be referred to herein, as “CORE.” CORE is stored in the Cloud and shared among the states and managed on each state’s instance. While most of the code is shared, each state manages their own instance of the code. As such, production deployments will often include updates to the core solution as well as all state specific code.
31. All environments for each state (production, development, and staging) reside in the Cloud. Currently, the Consortium exclusively uses AWS for Cloud Infrastructure. The Consortium reserves the right to switch to other Cloud Vendors at its discretion. There are no current plans to manage any hardware on premises so the Vendor should not consider managing in-house resources when pricing support.
32. The solution’s architecture is multi-instance. Each state controls its own instance. *Appendix H - Consortium System Overview* provides a System Overview.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

#### III. VENDOR REQUIREMENTS

33. MANDATORY requirements are clearly identified in this RFP. Failure to meet the MANDATORY requirements may cause a Vendor's bid to be unsuccessful. All other qualifications will count towards technical and key personnel requirements. The Vendor has the option to achieve these MANDATORY requirements through subcontracting/teaming agreements, if applicable. The Vendor must discuss or provide evidence of its asserted qualifications, experience, personnel, and/or abilities identified in this RFP to deliver the specified services herein.

#### A. Vendor Qualifications

34. The Vendor must demonstrate past (within the last ten (10) years) and current proficiency and experience using either or both of the technology stacks employed by the individual Consortium States.
35. The Vendor must demonstrate a recent track record of maintenance and support of a system the size and scope of the systems of each Consortium State as described in this RFP packet (namely, the existing technology state).
36. The Vendor must substantiate experience with two (2) prior projects (within the last ten (10) years) relevant to these criteria.
37. The Vendor must have demonstrated proficiency and experience in the design, development, and support of microservices and transforming monolithic apps into modular microservices using container technology.
38. The Vendor must have five (5) years of demonstrated proficiency and experience in developing applications for the cloud.
39. The Vendor and each Subcontractor must demonstrate financial strength to accommodate and support all the tools and sufficiently large workforce to independently handle the scope of the contract by submitting a letter of financial capability regarding the Vendor's working capital and workforce details in Section E. Staffing Plan
40. The Vendor must have demonstrated proficiency and experience of at least one (1) year in developing applications using AI, ML, U/X, C/X to enhance user experience.
41. The Vendor must demonstrate proficiency and experience of at least five (5) years' working with a state or federal government system.
42. The Vendor must specifically demonstrate its proficiency and experience, including the number of years and the scope of such experience, supporting, maintaining and/or developing a state UI system.
43. The Vendor must identify all executive and professional personnel to be assigned to the project, provide a summary of their qualifications, and a copy of their resume. Resumes must reflect qualifications and recent experience relevant to the scope of the work indicated in this RFP and the area of the project that the proposed individual will be assigned.
44. Background Checks: The Vendor must conduct criminal background checks and not utilize any staff, including sub-contractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

convicted of any felony or any misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The Vendor must promote and maintain an awareness of the importance of securing the State's information among Contractor's, employees, and agents. The Vendor must agree to allow their staff, including any subcontractors, to be subject to additional background checks performed by the State. The Vendor must describe the background verification process used in the hiring of its management staff and its individual consultants.

45. The Vendor must demonstrate proficiency in Agile development (preferably Scrum).
46. The Vendor must demonstrate proficiency and experience working with projects that involve collaboration with multiple customers, joint ventures, and/or infrastructure services companies.
47. The Vendor must demonstrate proficiency and experience managing applications in the AWS Cloud.
48. The Vendor must demonstrate proficiency and experience with Kubernetes, containerization, and data streaming.
49. The Vendor must demonstrate successful deployment of two (2) significant microservices projects within an enterprise application.

#### **B. Vendor Capabilities**

50. Project Management and Planning
  - a. Develop a comprehensive project work plan and Project Management Plan, including recommendations for staff, skills, equipment, training, and responsibilities.
  - b. Analyze and evaluate project progress, resources, budget, schedules, workflow, and reporting.
  - c. Review and analyze project management planning and software development documents.
51. Stakeholder Consultation and Requirements
  - a. Oversee product management and strategic planning to align with project goals and stakeholder needs.
  - b. Consult with stakeholders to assess user involvement and system functionality.
  - c. Sketching, wireframing, prototyping, and user task flow development.
  - d. Review and ensure traceability of business and technical requirements throughout the development and implementation phases.
52. Performance and Risk Management
  - a. Develop performance metrics to track project completion against milestones.
  - b. Provide risk management assessments and capacity planning services.
  - c. Conduct analysis of past project performance (schedule, budget) to identify and recommend improvements.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

53. Development Processes and Configuration Management
  - a. Review and monitor development processes to ensure they are documented and analyzed for improvement.
  - b. Assess and recommend improvements for Configuration Management (CM) practices and tools.
  - c. Oversee open-source software development and manage authentication services.
  - d. Implement and manage industry standard CI/CD processes to streamline development and deployment.
  - e. Refactor code to reduce technical debt and improve system maintainability.
  - f. Manage API development and documentation as part of configuration management.
54. Deliverables and Documentation Review
  - a. Perform detailed reviews of project deliverables, system documentation, software architecture, and application software for accuracy, completeness, and adherence to standards.
  - b. Analyze application, network, hardware, and software performance relative to expectations and industry standards.
55. Testing
  - a. Assess and recommend improvements for software testing adequacy, including review of test cases and direct observation of testing.
  - b. Automated testing (unit, integration, end-to-end).
  - c. Ensure that public-facing sites and tools are thoroughly tested to meet quality standards.
  - d. Assist with all facets of User Acceptance Testing (“UAT”) assistance. *i.e.*, test case identification, demonstration, data setup, defect and retest planning, and other necessary services to complete UAT.
56. Documentation and Training
  - a. Ensure appropriate end-user, administrator, and developer training is planned and executed.
  - b. Provide and/or update user manuals, help guides, and FAQ documents for users.
  - c. Provide and/or update operational runbooks and administrative guides.
57. Capacity and Usability Analysis
  - a. Review and analyze system capacity studies.
  - b. Conduct usability research, including contextual inquiry and stakeholder interviews.
  - c. Oversee content design and copywriting as part of usability research and ensuring effective user experience.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

#### C. Staffing Requirements

58. Company Profile and Key Resources
  - a. The Vendor must provide a company profile detailing the current number of employees available for the contract and key resources.
59. Employee Location and Reporting
  - a. **MANDATORY:** Onshore Resources: MDES allows only onshore resources to be utilized. Each Consortium state may elect to allow work to state specific code to be completed offshore; however, at no time may CORE work be performed offshore. CORE work support staff must be onshore. This is a mandatory requirement.
  - b. Monthly Status Reports: Provide monthly status reports to the PMO detailing employee location, skills, pending visa issues (if any), time-off requests that exceed one week, and position. The PMO may adjust reporting specifications as needed. Failure to timely deliver reports to the PMO may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
  - c. **MANDATORY:** Visa Issues: Describe if and how many employees the Vendor proposes to be assigned to this contract that are subject to visa requirements. For each of those employees, report the loss of any visa that impacts an employee's ability to continue CORE work immediately. The Vendor's employees may only continue to work if assigned to a state that allows offshore work and if the work is specific to that state. Otherwise, the Vendor must present its plan to provide a replacement for any of its employees who must leave the USA because of visa issues. This is a mandatory requirement.
  - d. Work site Approval: The Consortium State must approve work site locations other than the Consortium State's facilities. Remote Work and Hybrid work must meet all security requirements and be cost-effective and add value to Consortium State's. For MDES, the following Vendor key staff must be assigned to work on-site: Project Management Lead, Senior Architect, Business Analyst Leads, Test Lead, Quality Analyst, Database Administrator, Lead Developers.
    - A. Consortium State Facility Access
      - a. The Consortium States will provide facility access at their discretion and maintain virtual desktop infrastructure (VDI).
      - b. Each individual Consortium State shall establish secure access protocols for its respective state system.
      - c. Each individual Consortium State will assist the Vendor's employees with secure access to the CORE and an appropriate individual system, for both on-premise and remote workers.
      - d. **MANDATORY:** It is imperative that individual state confidential UI data shall never leave the United States under any circumstances. This is a mandatory requirement.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- e. **MANDATORY:** Vendor-provided equipment must meet each Consortium State's IT requirements including, but not limited to, security requirements. This is a mandatory requirement.
  - f. At the discretion of the individual Consortium States, each state may provide facility access to the Vendor's employees.
  - g. It is the individual Consortium State's decision to extend or to rescind privileges to each of the Vendor's staff members as it deems necessary.
  - h. If the privilege of working in state facilities is revoked, that Consortium State must provide reasonable notice.
  - i. If a Consortium State revokes facility privileges for a Vendor's staff member, the Vendor will retain only the necessary access to that state's system to fulfill the Vendor's obligations. However, in the case of imminent or immediate risk to MDES's system or the systems of the Consortium, the applicable state reserves the right to terminate the appropriate Vendor access forthwith.
- B. Remote Work Requirements
- a. The Consortium States will set specific restrictions and security requirements for remote work, with the Vendor responsible for related costs. For MDES, remote work schedules will only be approved under exceptional circumstances.
- C. Hybrid Work Requirements
- a. A hybrid work schedule will only be available under the following conditions: (1) written approval by the applicable Consortium State, and (2) shall be immediately revocable at the Consortium State's discretion. The Vendor's employees and subcontractors must report to the Consortium State(s)' state facility upon request. For MDES, hybrid work schedules will only be approved under exceptional circumstances.
- D. Each Consortium State reserves the right to revoke the Vendor's employee's facility access and adjust access as needed at any time and with no notice for violations of facility, security, or other state policies. The Vendor's employees and subcontractors must report to the Consortium State(s)' state facility upon request.
- E. Any exemptions from the worksite requirements must be approved by the Project Management Officer (PMO). If the Vendor disagrees with the PMO's decision, the Consortium Executive Committee (CEC) will receive and consider any requests for reconsideration and issue a final decision on the matter.
60. Staff Size and Workforce Management
- a. **Staffing Specifications:** The Vendor must specify the number of staff to be assigned post-award and provide a list of skills and credentials for the proposed staffing model.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- b. Workforce Payment: Each individual Consortium State will only pay for completed authorized work, not headcount. Estimates for the proposed scope of work should correspond to projected, completed authorized work.
  - c. Scaling: The Vendor must describe how it plans to scale up or down to meet demand but bill only for approved hours used.
  - d. Sprint Velocity: Baseline sprint velocity after 180 days; Each individual Consortium State will notify the Vendor of adjustments needed for demand fluctuations.
  - e. The Vendor will maintain capacity for all defect remediation work related to the CORE and state specific code, queries, and analyses. See paragraph 110 below for details on historical defect volume.
61. Employee/Vendor Removal
- Resource Removal: Each individual Consortium State may also request the removal of any Vendor resource without notice. The Vendor must replace the resource promptly without undue delay.
62. Employment Mix
- a. Employee vs. Staff Augmentation Ratio: The Vendor must maintain at least 70% of its own employees with a maximum of 30% contract employees.
  - b. Modification Requests: The Vendor must submit plans for changes in the employee/subcontractor ratio no later than thirty (30) days prior to any alteration. The PMO will review and approve such changes.
63. Security and Confidentiality
- a. **MANDATORY:** Compliance: The Vendor must adhere to all security, confidentiality, and other contract requirements of each individual Consortium State. This is a mandatory requirement.
64. Capacity Plan
- a. The Vendor must illustrate how it will start at 50% capacity.
  - b. The Vendor must reach 80% capacity within ninety (90) days of the contract start date and 100% within one hundred and eighty (180) days.
65. Key Positions
- a. The Vendor must include key positions in the staffing plan, ensuring they are Vendor employees unless otherwise permitted in writing by an individual Consortium State. Key employees must be full-time and reside in one of the Consortium states at least 50% of the time. Key positions should be dedicated and not shared with any other duties, though one person may hold multiple key positions if approved, in writing, by the individual Consortium State. The Vendor's plan must include the following:
    - A. Notice for Key Positions: Provide two (2) weeks' notice before replacing a key resource and supply credentials of replacements for Consortium State and PMO approval. The Vendor shall not reorganize key positions, including, but not limited to, moving to the same position with another state's UI agency without the written consent of MDES/Consortium.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- B. The Vendor must advise the appropriate Consortium member state(s) of any key position that is vacated within five (5) business days.
- C. The Vendor must replace any key position that is vacated for any reason within 60 days and advise the Consortium member state(s) of any replacement for a key position within thirty (30) business days of the planned start date.
- D. The appropriate Consortium Member state(s) shall have the right to review the credentials and experience of any replacement employee proposed to fill a vacant Vendor key personnel position and the right to refuse any candidate presented by the Vendor as a replacement. The appropriate Consortium member state(s) and the PMO shall have fifteen (15) days to review the candidate and provide the Vendor with a response.
- E. The Vendor must designate or assign within five (5) business days, an individual to serve as an interim for key positions that are vacated and notify the appropriate Consortium member State(s) within that same timeframe.
- F. Key Positions will be required to attend various offsite meetings and conferences as directed by MDES/the Consortium.
- G. The Vendor will provide resumes for all proposed key positions for each Consortium Member State(s).
- H. Minimum Key Positions: Included roles are:
  - a. Product/Program Manager – Responsible for oversight of the products being developed and maintained by the Consortium State(s).
  - b. Project Manager Lead – Responsible for leading the Vendor project team and coordinating with stakeholders to organize, track, and execute work.
  - c. Senior Architect – Responsible for designing, overseeing, and guiding the architecture of the application.
  - d. Business Analyst Leads – Responsible for overseeing the business analyst process for the application development process. Business Analyst Leads are required for both the tax and benefits side of the application in each Consortium Member state.
  - e. Quality Analyst – Responsible for overseeing the Quality Assurance process for the application.
  - f. Test Lead – Responsible for overseeing the System Testing process for the application and assisting Consortium Member States with User Acceptance Testing needs.
  - g. Lead Developers – Responsible for leading a team to design develop and maintain the application. They are responsible for serving as the technical leader within the development team. Lead developers are required for both the tax and benefits side of the application in each Consortium Member state.
  - h. Database Administrator – Responsible for ensuring that the database effectively supports the functionality and data needs of the application.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

Their focus is primarily on the design, maintenance, and performance optimization of the databases specifically used by application development teams.

- i. Backup/Disaster Recovery Administrator – Responsible for designing, implementing, and managing the disaster recovery strategies of the application system. These responsibilities may include but are not limited to: assessing application vulnerabilities, developing application Disaster Recovery Plans, Designing recovery architectures, Testing and Validation of application Disaster Recovery plans, monitoring application performance for potential issues that could impact recovery capabilities, leading incident response teams, overseeing data backups, management of data replication, ensuring data consistency for timely recovery, and collaborating with application developers to integrate disaster recovery considerations into new application development projects.
  - j. Security and Compliance – Responsible for overseeing the security practices within the application. These responsibilities may include but are not limited to: Conducting regular security reviews of applications to identify potential vulnerabilities and risks including code reviews, penetration testing, and threat modeling, ensuring applications comply with relevant data privacy regulations and industry standards, collaborating with developers to embed security practices into the development process, including secure coding standards, input validation, and access control mechanisms, and working with the appropriate Consortium State(s) regarding all security and compliance requirements.
  - k. Analytics/ Reporting – Responsible for overseeing the development and implementation of data analytics and reporting systems within an application development team. These responsibilities may include but are not limited to defining data collection and storage strategies, designing and building dashboards, reports, and visualizations to present key application development metrics, conducting in-depth analysis of application data to generate actionable insights for Consortium Member State(s), and collaborating with Consortium Member State(s) to identify their data needs.
66. Holidays - The Vendor must advise MDES / Consortium State(s) of any holidays (e.g., religious, cultural, etc.) other than Consortium State holidays that may result in the absence of three (3) or more employees, subcontractors or any key position. The Vendor must send notice of the applicable holidays fourteen (14) days in advance of any such holidays and must include the names of affected employees, subcontractors, or any key position. Failure to timely notify MDES / Consortium State(s) may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-011.
67. Vacations - The Vendor shall notify MDES / Consortium State(s) at least fourteen (14) business days prior to any employee's or subcontractor's scheduled vacation with a duration of more than five (5) business days and provide the name of the individual who is serving in this role during the interim. Failure to timely notify the

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

appropriate Consortium State(s) may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-011.

68. Subcontracting Plan
- a. Subcontractor Integration: Provide a subcontracting plan detailing how subcontractors will integrate with the prime staff as well as meet the following requirements.
    - A. **MANDATORY:** Offshore Subcontractors: Offshore subcontractors are not permitted by the existing Consortium States. MDES allows only onshore resources to be utilized. Each Consortium state may elect to allow work to state specific code to be completed offshore; however, at no time may CORE work be performed offshore. CORE work support or subcontractor staff must be onshore. This is a mandatory requirement.
      - i. A future Consortium state may approve offshore subcontractors for non-CORE work.
    - B. Key Personnel: Key personnel must be employees from the Vendor's staff unless otherwise permitted in writing by an individual Consortium State.
    - C. Subcontractor Ratio: Maintain the same employee to subcontractor ratio as stated in the Vendor's proposal unless otherwise permitted in writing by an individual Consortium State.
    - D. Subcontractor Approval: MDES/Consortium must approve all subcontractors unless identified in the initial proposal. All subcontractors must conform to contract requirements.

#### IV. DEVELOPMENT PRACTICES

##### A. Agile Development Practices

69. The Consortium and Vendor will participate in Agile ceremonies (sprint planning, daily stand-up, sprint review, retrospective, etc.) and will reach an agreement on the definition of the following: story points, sprint cycles, release schedules, definition of done, and sizing of epics, stories, and tasks. The Vendor shall discuss its plan for this process.

##### B. Required Product Release Processes

70. Definitions
- a. Release - the delivery of a product or service increment into a production-quality environment, such that it is available for immediate use by stakeholders.
  - b. Change Impact Analysis - a process for defining, evaluating, and measuring how changes in an application can affect other parts of the system. Change impact analysis shall be interchangeable with impact assessment for this project.
  - c. System Use Case (SUC) - sequence of actions a system performs that yields an observable result of value to a particular user.
  - d. System testing - a process that verifies that the software performs as designed and meets the requirements that guided its development. System testing identifies discrepancies between the actual system and its intended



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- functionality including bugs, errors, or missing requirements. System testing is performed by the Vendor prior to user acceptance testing.
- e. Product or Sprint Demonstration - is presentation of a product by the development team to show stakeholders the developed product and to allow feedback for any missed requirements or unexpected performance items.
  - f. User acceptance testing - is a phase of software development that ensures the developed product meets the users' needs, satisfies all requirements, and performs as expected.
71. Product Release Requirements – These requirements shall be performed before each product is moved to a production release.
- a. Any of the following requirements to move a product to release may be waived by an individual Consortium state at their sole discretion. Any waiver by a single state shall not apply to other participating states for multiple state deployments.
  - b. The Vendor will perform a Change Impact Analysis.
  - c. The Vendor will provide SUCs to the Consortium State(s).
  - d. The Vendor will perform System Testing and provide the Consortium State(s) with detailed results, including screen shots, of said testing. The Vendor will also provide a report at the conclusion of system testing showing the automated test coverage percentage, number of automated test cases performed, and total number of test cases performed during system testing for that product. Failure to provide the required report for any product may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
  - e. The Vendor will conduct a product demonstration of all new products prior to releasing the product to user acceptance testing.
  - f. The Vendor will release the product into User Acceptance Testing a minimum of fourteen (14) days before a production release to ensure time for Consortium State(s) to adequately perform user acceptance testing.
  - g. The Vendor shall not release a product to production without the Consortium State(s) official approval. This approval requires completion of a product demonstration and completed user acceptance testing.
  - h. The Vendor will create or update user manuals for changes made to the system including but not limited to screen changes, functionality changes, or role/access changes.
  - i. The Vendor, as a part of the product release requirements, will at the completion of each product, provide a final product report showing the following items and attach it to the final invoice for that project.
    - A. Date Change Impact Analysis was completed.
    - B. Date system testing was completed.
    - C. Date system testing results were shared with the Consortium State(s).
    - D. Date of product demonstration and list of attendees of the product demonstration.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- E. Date that the product was released to user acceptance testing.
  - F. Date of the completion of user acceptance testing and approval documentation.
  - G. Date of the release to production.
  - j. Failure to provide the final product report for any product may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
72. The Vendor must follow the product release requirements for any product change or addition to the ReEmployUSA system regardless of whether this is a single or multiple state deployment.
73. Failure to follow the product release requirements for any product may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-016.

#### V. SOCII AUDITS

74. SOCII audits are a requirement for this award. The Vendor is responsible for completing a yearly SOCII audit. As part of its plan for this audit, the Vendor must, at a minimum, include the following:
- a. The Vendor is responsible for completing the audit within the first ninety (90) days post award.
  - b. The Vendor is required to complete the audit within a 180-day timeframe from start to finish.
  - c. At the request of each Consortium State, the Vendor shall be prepared to evaluate and propose a firm to complete the audit for the appropriate Consortium State's approval.
  - d. Consortium States will dictate the type of audit to be conducted.
  - e. Consortium States will own all the information from the audit and can participate in the audit to whatever level deemed necessary or appropriate.
  - f. Failure to complete a timely annual SOCII audit may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.

#### VI. PLANNING

75. The following three (3) plans, Enterprise Architecture Plan, Development and Quality Management Plan, and Information Data Security Plan are expected to be delivered to Consortium States within 180 days post award for approval. The Vendor must provide a baseline framework of the required three (3) plans within forty-five (45) business days of the award. The Vendor must provide a draft Transition Plan as part of its Narrative Response to this RFP. This baseline framework will include a Deliverable Expectation Document, outlining by section a proposed plan with details for all major deliverables (documents). The Disaster Recovery Plan is expected to be delivered to the Consortium States within thirty (30) business days post award for approval. In response to the RFP, the Vendor must demonstrate readiness to provide the following plans within the 180-day/45-day/30-day timelines and at the intervals noted. The Vendor agrees to alter the plan as required by the Consortium States to arrive at a product conducive to development needs of the Consortium States Failure to complete the post award

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

plans timely result in a penalty assessment. See Table 10 Post-Award Maximum Penalties.

#### A. Enterprise Architecture

76. Enterprise Architecture - The Vendor will baseline the current Enterprise Architecture (EA) of each of the Consortium States framework and work with the Consortium States to create a roadmap to enhance EA. The roadmap will be based on a three (3) to five (5) year period (three (3) year period preferred) applying industry trends where appropriate to deliver best-in-class performance.
- a. The Vendor will document, build, and deliver transition architectures from the current state to the proposed state. (“Technical Roadmap”).
  - b. The Vendor will work with each state’s Technical/Business Team to capture, document, and deliver the Technical and Business Roadmaps. The Technical Roadmap must complement the Business Roadmap.
  - c. The Vendor will work with MDES and the Consortium States to outline progress towards goals and re-baseline the roadmap based on completions and industry trends.
  - d. The Framework can be based on any of the industry standard frameworks, for example, TOGAF, Zachman, ITIL, Gartner, or Microservice. The Consortium States must authorize the framework prior to finalizing the plan.
  - e. The architecture will include the use of automation functions to the greatest extent possible to drive business outcomes on the roadmap.
  - f. The document should highlight how each provision adds value to the Consortium States.
  - g. The Vendor will review, update, and deliver both the “technical roadmap” and the “business roadmap” every 180 days to ensure consistency with current technologies. The Vendor will communicate all changes as they occur.
  - h. Failure to timely deliver updated technical and business roadmaps may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.

#### B. Development and Quality Management Plan

77. The Vendor shall design, code, and test according to development standards approved by the Consortium States while keeping quality at the forefront of all development and support of the ReEmployUSA system. Development standards shall follow the requisite style guide (Java or Angular) and be a comprehensive roadmap throughout the software development lifecycle. The Development and Quality Management Plan will detail how the Vendor plans to deliver architectural documents, wireframes, schemas, and other design documents in the process of supporting or enhancing the system as well as serving as the guide for the Vendor to meet quality requirements. The plan will detail triggers for modifying and upgrading documents as well as the level of detail required to achieve traceability.
78. The Vendor will, as a required component of project and support management, keep documentation up to date as required in the EA plan. The Vendor will update any documentation that is found either internally or by any Consortium State to be outdated due to changes created by the Vendor to begin no later than one (1)

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

month after such discovery. Further, the Consortium States may penalize the Vendor for omitting document creation/updates as required.

- a. Code Modularity – The Vendor will understand and employ code modularity to reduce complexity and make code more efficient, reliable, and maintainable. The Vendor will recommend a baseline for each standard based on experience and industry standards.
  - b. Compliance - The Vendor’s plan will guide development services in a manner that ensures that all applicable state, federal, legislative, and regulatory requirements are met in the design, development, and implementation of any ReEmployUSA functions. Likewise, the designs must comply with any non-federal or state audits and controls.
  - c. Batch Processing Alternatives - New designs will limit the use of batch processing to the greatest extent possible. The Vendor’s designs should favor alternative methods such as streaming to reduce the workload of maintaining batch operations. The Vendor should also recommend a plan for removing/modernizing existing batch programs.
  - d. Security - The Vendor will propose the use of standards aligned with industry best practices. Reliance on third party security tools shall be discouraged, and the Vendor will develop these items with native tools to enhance security posture for each state’s system.
  - e. Software Architecture Plan- The Vendor will develop a Software Architecture plan that will align with the Enterprise Architecture Strategy to guide development efforts to evolve towards microservices and industry best practices with reference to those specific practices that will be updated as appropriate. The proposed strategy will focus on how to scope functions, trade-offs to the approach, security solutions, Application Programming Interface (API) implementation, along with management, and growth of the plan.
79. The Development and Quality Management Plan will at a minimum address the following:
- a. Roles and responsibilities of all parties involved
  - b. Design, development, and testing of the ReEmployUSA system.
  - c. Testing plan detailing each level of testing, the criteria, personnel required, and necessary remediations.
  - d. Metrics on monitoring and controlling quality.
  - e. A description of quality services and tools.
  - f. List and description of all deliverables and products.
  - g. Development Standards and methodologies.
  - h. Evaluation and reports to MDES/Consortium States.
  - i. Quality Standards: Define the criteria for data quality (accuracy, completeness, consistency). Validation and Cleansing Procedures:
    - i. Detail methods for data validation, error detection, and data cleansing.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- j. Monitoring and Reporting: Explain how data quality will be monitored and how issues will be reported and addressed.

#### C. Information Data Security Plan

- 80. The Vendor will develop, deliver, and maintain an Information Data Security Plan that ensures compliance with current industry standard requirements, such as NIST 800-53 Rev 5, IRS Publication 1075, SSA requirements, and 20 CFR 603. This plan will include the process to protect and maintain data confidentiality and integrity and implement security controls. The controls must focus upon the prevention, detection, and correction of security events.
  - a. The Vendor will develop the Information Data Security plan that the Consortium States shall review and approve before adoption. The plan will include all tools, software, and security mechanisms currently utilized by the Consortium States.
  - b. The plan will be created using industry standard best practices to employ security controls that protect the MDES/Consortium States against threats to the ReEmployUSA system.
  - c. The plan will illustrate how the Vendor will incorporate security into every facet of the requisite Software Development Lifecycle.
  - d. Information Data Security procedures employed will protect MDES/Consortium States when the Vendor access to the state system is required for contracted functions.
  - e. Information Data Security procedures employed will comply with the requirements specific to each individual consortium state's Information Technology Agencies as required. For MDES these procedures are:
    - A. Information Technology Service's Enterprise Security Policy (<https://www.its.ms.gov/sites/default/files/ServicesPDFs/10-1-2013%20ESP.pdf>),
    - B. Information Technology Service's Enterprise Cybersecurity Incident Reporting Guidelines ([https://www.its.ms.gov/sites/default/files/ServicesPDFs/Enterprise%20Cybersecurity Incident Reporting 23-24.pdf](https://www.its.ms.gov/sites/default/files/ServicesPDFs/Enterprise%20Cybersecurity%20Incident%20Reporting%2023-24.pdf)), and
    - C. Miss. Code Ann. § 25-53-201.
  - f. The Vendor's plan will detail how services will maintain compliance with all current audit requirements to include the SOC2 Type2 audit.
  - g. Maintenance of the Information Data Security Plan requires that this plan be updated within 30 days of any change, alert, or release of guidance by the IRS, SSA, NIST, or an individual state(s) Information Technology Agency.
  - h. Failure to deliver an updated Information Data Security Plan time may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
- 81. The component requirements of the information data security controls shall present a solution for:

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- i. Access Controls - role-based security, physical security, and remote access
  - ii. Procedural Controls - training, contingency planning, and incident response planning
  - iii. Technical Controls - hardware and software components that aid in the prevention, detection, and protection of systems against a cyber-attack
  - iv. Administrative controls - Vendor's plan to lead and govern its team
  - v. Baseline Confidentiality Controls:
    - A. Gap analysis on existing systems and tools used for data protection and fraud prevention
    - B. Audit security roles and Personally Identifiable Information (PII)/ Federal Tax Information (FTI) access
    - C. Controls to prevent the Vendor from any access to FTI data
    - D. Description of PII usage in various environments detailing where PII is prohibited and procedure to accomplish development tasks without the use of PII.
    - E. Description of FTI usage in various environments detailing where FTI is located.
    - F. The Vendor should present an approach within the monitoring plan that identifies patterns inconsistent with normal practices which may uncover illicit Service, both internal and external.
82. The following outline may serve as a guide or reference for the Vendor response.
- i. Introduction
    - A. Purpose and Scope: Describe the objectives of the Information Data Security Plan and its relevance to the agency's mission.
    - B. Project Overview: The Consortium State will provide background on its project, including goals and expected outcomes to assist the Vendor with the creation of this plan.
  - ii. Data Governance Framework
    - A. Roles and Responsibilities: Define roles such as data owners, stewards, and custodians, along with their responsibilities.
    - B. Policies and Standards: Document the data governance policies, procedures, and standards that will be followed.
  - iii. Data Architecture and Infrastructure
    - A. Data Sources and Types: List all data sources, types (structured, unstructured), and formats.
    - B. Data Storage Solutions: Describe where and how data will be stored (e.g. cloud storage).
    - C. Integration with Existing Systems: Explain how the data management system will integrate with current agency systems.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- iv. Data Collection and Ingestion Processes
  - A. Data Acquisition Methods: Detail how data is collected, including any tools or technologies used.
  - B. Ingestion Pipelines: Describe processes for importing data into systems, including ETL (Extract, Transform, Load) procedures.
- v. Data Security and Privacy
  - A. Security Measures: Outline the strategies for protecting data, including encryption, firewalls, and access controls.
  - B. Compliance with Regulations: Explain how the plan ensures compliance with laws and regulations including IRS Publication 1075, FTI requirements and state-specific regulations.
  - C. User Authentication and Authorization: Describe how users will be authenticated, what authorization levels will be in place and how authorization levels are defined.
- vi. Data Lifecycle Management
  - A. Lifecycle Phases: Describe each phase of the data lifecycle from creation to deletion.
  - B. Retention Policies: Specify data retention periods based on data types and regulatory requirements.
  - C. Archiving and Disposal: Outline processes for data archiving and secure disposal.
- vii. Metadata Management
  - A. Metadata Standards: Identify standards for metadata to ensure consistency and usability.
  - B. Cataloging and Indexing: Explain how metadata will be cataloged and indexed for easy retrieval.
  - C. Metadata Utilization: Describe how Metadata will support data discovery and governance.
- viii. Data Access Sharing
  - A. Access Controls: Define who has access to what data and under what conditions.
  - B. Data Sharing Protocols: Outline procedures for sharing data internally and externally.
  - C. User Interface (UI) Design Considerations: Document how the User Interface will facilitate data access while ensuring security and compliance.
- ix. Backup and Recovery Plans
  - A. Backup Procedures: Detail the backup schedule, methods, and storage locations.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- B. Disaster Recovery Strategy: Provide a plan for data recovery in case of system failure or other disasters.
- C. Testing and Maintenance: Describe how backup and recovery processes will be tested and maintained.
- x. Compliance and Audit
  - A. Regulatory Compliance Mapping: Map data management practices to specific regulatory requirements.
  - B. Audit Trails and Logging: Explain how services will be logged for auditing purposes.
  - C. Reporting Mechanisms: Detail how compliance reports will be generated and disseminated.
- xi. Risk Management including Cyber Risk Management
  - A. Risk Identification: List potential risks.
  - B. Mitigation Strategies: Propose measures to mitigate identified risks.
  - C. Incident Response Plan: Outline procedures for responding to data breaches or other security incidents.
- xii. User Training and Support
  - A. Training Programs: Describe training initiatives for staff on data management policies and tools.
  - B. Documentation and Resources: Provide user manuals, guidelines, and other support materials.
  - C. Helpdesk and Support Services: Explain how users can get help with data management issues.
- xiii. Implementation Roadmap
  - A. Timeline and Milestones: Present a schedule for implementing the Information Data Security Plan components.
  - B. Resource Allocation: Detail the human, technical, and financial resources required.
  - C. Change Management Plan: Outline strategies for managing changes during implementation.
- xiv. Monitoring and Continuous Improvement
  - A. Performance Metrics: Define key performance indicators (KPIs) for data management.
  - B. Monitoring Processes: Describe how data management services will be monitored.
  - C. Feedback Mechanisms: Explain how feedback will be collected and used to improve the Information Data Security Plan.

#### **D. Transition Plan**



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

83. The successful Vendor shall have a Transition Plan to assist the Consortium States in their shift to the new contract. A seamless transfer to the new contract with the successful Vendor, whether new or existing, is in the best interest of the public.
84. The plan shall specify the timeline for the transition, tasks to be performed by the parties, the schedule for the performance of such tasks and the respective responsibilities of the parties associated with the identified tasks. The plan should include at a minimum: data migration, communication, operational continuity, training and support, risk management, evaluation and feedback, and documentation. The plan should enumerate potential risks with the transition. This plan must demonstrate that the Vendor has the capacity and demonstrated competency to assume ownership of the Maintenance and Support of ReEmployUSA without any reliance on the incumbent Vendor.

#### E. Disaster Recovery Plan

85. As part of the overall Disaster Recovery Plan (DRP), the Vendor shall:

Develop a Baseline Update Form for the ReEmployUSA Disaster Recovery Plan. See *Appendix B - Disaster Recovery Response Plan*. The content of the baseline update shall be developed in collaboration with the MDES/Consortium States and its Cloud Services Provider.

  - a. Use the Consortium States template for the updated Plan. *Appendix B - Disaster Recovery Response Plan*– Consortium Disaster Recovery Plan provides the current template. The updated form/report is due within 30 business days of the start of the contract and must meet the documentation standards of the Consortium States (also referred to as, “the Consortium”). Elements of the Disaster Recovery Plan:
    - i. Disaster Recovery Training
    - ii. Performance & Reporting for Failover Testing
    - iii. Performance & Reporting for Fallback Testing
    - iv. Environments Work Plan
    - v. Performance of Disaster Recovery Plan

#### VII. DEFINITIONS

86. Scope of Services for this RFP is defined as all Corrective Maintenance Services, Adaptive Maintenance Services, Preventive Maintenance Services, Perfective Maintenance Services, and Support Services for all of these types of maintenance services.
87. Maintenance and Support is defined as the comprehensive management of the ReEmployUSA application which includes all work that is NOT a Perfective Maintenance Service. Maintenance and Support will include all Adaptive Maintenance Services, Corrective Maintenance Services, Preventive Maintenance Services, and support services for all of these types of maintenance services. The Vendor will provide a Maintenance and Support Services fixed cost price per Consortium State in *Attachment C - Cost Information Submission Form* of this RFP.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

88. Support Services or Production Support Services are defined as maintaining and ensuring the smooth operation of a live software application. Support/Production Support services include but are not limited to, writing and executing queries, troubleshooting issues, analysis, resolving problems, monitoring system performance and security, disaster recovery, database recovery, optimizing database performance, running and re-running reports, running and re-running batches, system administration, support ticketing, interfaces with other systems, training, entering, removing, or changing data stored in existing database tables, and generating reports on incident trends, potential risks, or system performance.
- Support Services or Production Support Services will include working with other Vendors and state support staff. All support services are included as a part of the scope of service of this RFP. The Vendor will include ALL support Services in the Annual Maintenance and Support Services fixed cost price per Consortium State provided in *Attachment C - Cost Information Submission Form* of this RFP.
89. Corrective Maintenance Services are defined as identifying and resolving defects. These defects include but are not limited to coding errors, design flaws, software dependency issues, security vulnerabilities, performance issues, usability issues, or integration issues. Proper documentation of changes done is a part of corrective software maintenance, and all corrective maintenance services are included as a part of the scope of service of this RFP. The Vendor will include ALL Corrective Maintenance Services in the Annual Maintenance and Support Services fixed cost price per Consortium State provided in *Attachment C - Cost Information Submission Form* of this RFP.
- a. A defect is a failure, flaw or error that results or functions in unexpected, incorrect, or unintended ways in system testing (ST), user testing (UAT) or production environments.
90. Preventive Maintenance Services are defined as identifying and resolving potential problems before they become major issues. This includes but is not limited to performance management, optimizing data, cleaning up unnecessary files, tables, etc., backing up data, reviewing system logs for potential issues, software updates (regardless of type), addressing known security vulnerabilities and bugs, code refactoring, cleaning of codes, documentation updates, updating libraries and frameworks, reviewing code quality, and updating system configurations for optimization. All preventive maintenance services are included as a part of the scope of service of this RFP. The Vendor will include ALL Preventive Maintenance Services in the Annual Maintenance and Support Services fixed cost price per Consortium State provided in *Attachment C - Cost Information Submission Form* of this RFP.
91. Adaptive Maintenance Services are defined as the modification, revision, and / or updating of application software, interfaces, APIs, etc. (non-exclusive list) to remain current with changing environments or changes to infrastructure. Environmental changes include, but are not limited to, patches, minor upgrades, or major upgrades of operating systems, software dependencies, network changes, security upgrades, changes in external systems, and system configurations. Additional adaptive maintenance services include planning, coordinating, troubleshooting, remediation of issues or build deployments necessary to maintain current functionality that are due to changing environments
-

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

or infrastructure. All adaptive maintenance services are included as a part of the scope of service of this RFP. The Vendor will include ALL Adaptive Maintenance Services in the Annual Maintenance and Support Services fixed cost price per Consortium State provided in *Attachment C - Cost Information Submission Form* of this RFP.

92. Perfective Maintenance Services are defined as development, installation, or integration of additional features or requirements needed to enhance the system. This includes but is not limited to adding new features, improving existing features, and updating user interfaces for enhanced usability. Perfective Maintenance shall also be known as enhancements in this RFP. All Perfective Maintenance Services are included as part of the required scope of service of this RFP. However, Perfective Maintenance Services are NOT included as a part of monthly maintenance and support, but must be costed and bid separately from the monthly Maintenance and Support cost through either a Fixed Cost SOW using the Fully-loaded Hourly Perfective Maintenance Service Statement of Work Rate, or Time and Materials estimate using the Fully-loaded Hourly Time and Materials Rate. In both cases the Vendor must provide the estimated number of professional service hours that will be necessary to implement the work contemplated therein.
93. Fixed Cost is defined as an agreed upon cost for the scope of work defined using the corresponding fully-loaded rate.
  - a. Fixed cost pricing will be used for the Annual Lifecycle Maintenance and Support fee that will be broken into monthly payments.
  - b. For MDES, all SOWs will be fixed cost projects using the Fully-loaded Hourly Perfective Maintenance Service Statement of Work Rate unless approval for the specific project has been given to perform using T&M or the project will be forty (40) hours or less.
  - c. For MDES, all Change Order SOWs will be fixed cost using the Fully-loaded Hourly Change Order SOW Rate.
94. Time and Materials (T&M) is defined as a predetermined, agreed upon Fully-loaded Hourly Time and Materials Rate which will be used to calculate the payment for services provided by the Vendor plus any materials used under a project charged as T&M. Subject to the definitions and provisions herein.
95. Shared Services are defined as the CORE services delivered by individual Vendor staff to either multiple Consortium states and/or on shared Consortium projects.
96. Statement of Work (SOW) is defined as a document outlining the scope, requirements, assumptions, timeline, deliverables, milestones, estimated number of professional service hours that will be necessary to implement the work contemplated therein and cost of a project required by one or more Consortium State(s).
97. A Change Order is defined as a statement of work (“CO-SOW”) setting forth in reasonable detail, the range and extent of services requested, requirements, assumptions, timeline, deliverables, milestones, estimated number of professional service hours that will be necessary to implement the work contemplated therein, and cost of a project requested by one or more Consortium State(s) that would

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- expand the scope of services of this project. A Change Order would require approval from ITS.
98. Sensitive Data is defined as any information that is protected against unwarranted disclosure by state and/or federal laws or regulations. Sensitive Data includes but is not limited to personal information (PI), personally identifiable information (PII), Federal Tax Information (FTI), sensitive personal information (SPI), nonpublic personal information (NPI), and Material Nonpublic Information (MNPI), financial data, and business-specific sensitive data.
  99. Cyber Attack is defined as a successful attempt to compromise the security, integrity, or availability of ReEmployUSA or the data within as per Miss. Code § 25-53-201(5)(a), as amended.
  100. Cyber Security Incident is defined as any Service that could potentially harm system security, including attempted and unauthorized access, malware detection, suspicious Service, or configuration errors. See Miss. Code § 25-53-201, as amended.
  101. Breach is defined as the successful penetration of a system's security where unauthorized access has occurred even if the underlying data has not been accessed.
  102. Data Breach is defined as the exposure, disclosure, alteration, destruction, or theft of sensitive data.

#### **VIII. PERFECTIVE MAINTENANCE SERVICES / ENHANCEMENTS**

103. Any Perfective Maintenance Services requested under this RFP and the contract with the successful Vendor shall include the preparation of a T&M estimate or of a Fixed Cost SOW (as specified by each individual Consortium State) using the proper fully-loaded hourly rates as presented in *Attachment C - Cost Information Submission Form*. The Consortium States shall not pay for estimates or SOWs regardless of whether the perfective maintenance service requested is ultimately accepted. Preparation of the T&M estimate or SOW does not bind the Consortium State to selection of this Vendor for this project. The Vendor should view these documents as bids for this project.
104. This RFP will not be the exclusive vehicle for the Consortium to engage a Vendor for perfective maintenance services. The Consortium may, at its discretion, perform any part of this work in-house or through another Vendor.

#### **A. Perfective Maintenance Service Volume**

105. The Consortium engages in projects to continually modernize the system. In addition to modernization and system optimization, a portion of perfective maintenance services result from public emergencies and new or updated state and federal requirements. The volume of perfective maintenance services relates directly to federal and state funding, state and/or federal law changes, external conditions, emergencies, upgraded system functions, and efficiency of Vendor performance.
  - a. It is anticipated that perfective maintenance services work will be between 80 and 120 user stories per month for the Consortium. A user story is an informal, general explanation of a software feature written from the perspective of the

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

end user. Its purpose is to articulate how a software feature will provide value to the customer. These anticipated perfective maintenance services are evenly distributed.

- b. Implementation of new federal or state programs may occur at any time, are outside of the control of the Consortium, and are mandatory for the states to implement, usually by a specific deadline.
- c. New federal or state funding opportunities may occur at any time, shall be sought out by the individual Consortium State(s) at their sole discretion, contain strict timelines, and if received by the Consortium State(s) are mandatory.

#### **B. Anticipated Perfective Maintenance Services**

106. The Vendor should present proposed solutions for perfective maintenance services either consistent with the current initiatives or with innovative alternatives. The cost for these anticipated perfective maintenance services must NOT be included in the costs provided for this RFP. A request for a fixed cost SOW or T&M estimate will be requested if any Consortium State wishes to proceed with these proposals at a later time. Current initiatives underway and the goals of each include:

- a. Microservices & Modularity – Develop apps more rapidly and allow greater portability of the apps.
- b. Artificial Intelligence (AI)/BOTS – Utilize BOTS (RPA and others) and AI to reduce manual workloads and streamline processes without human intervention. *Appendix F - MDES Artificial Intelligence Governance Policy* explains the permissible and prohibited requirements for use of AI for this agency.
- c. Mobile Technology – Enhanced apps should deliver better responsiveness while accommodating customer’s expanding use of mobile devices.
- d. Reporting – Increase self-service analytics, adapt fraud analytic tools, and move to more agile analytic tools.
- e. Interactive Voice Response (IVR) – Utilize customer data known by the system to integrate with call center functions using artificial intelligence or other tools to provide an enhanced user experience, focusing on interoperability of the systems.

#### **C. Perfective Maintenance Service Approval Process**

107. The State will determine if the perfective maintenance service is a part of the Scope of Services of this RFP. If it is not, the State will initiate a Change Order with ITS. If it is, the State will utilize the following processes.

108. The Consortium will utilize a process where any member state may initiate a perfective maintenance service.

109. Perfective Maintenance Service Consortium Voting Process.

- a. The member states will hold a first vote on the proposal.
- b. Each state may elect to Approve or Abstain. If the state abstains, the state indicates that it is uninterested in that project.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- c. The Vendor will then gather the requirements of the project and present a timeline and cost for the perfective maintenance service in both of the following formats.
    - i. T&M or
    - ii. Fixed Cost SOW
  - d. Each member state will then vote again to Approve, Disapprove, or Abstain.
  - e. States that previously abstained or disapproved with the first vote may decide to approve for the second vote, and states who previously approved may decide to abstain for the second vote.
  - f. If an additional state approves the perfective maintenance service upon the second vote, the Vendor will need to gather any additional state specific requirements.
  - g. Approval of a perfective maintenance service does not indicate participation in the project. At its sole discretion, a state may approve a project but may not be able or willing to go forward with that project at that time. In those circumstances, the other state(s) will proceed with the cost split among those states approving and agreeing to participate in the perfective maintenance service.
110. Perfective Maintenance Service Cost and Service Approval Process
- a. Each individual Consortium State may elect to approve the Service using either the T&M cost method or a Fixed Cost SOW method. The Consortium members are not required to utilize the same costing method for any perfective maintenance service.
    - i. For MDES, all perfective maintenance services with an estimated timeline of more than forty (40) hours must have a SOW, while perfective maintenance services with an estimated timeline of forty (40) hours or less may be presented using T&M. This requirement shall be followed unless expressly waived by this state.
    - ii. For MDES on CORE projects, the Vendor must present a complete SOW or T&M estimate with the costs split by state and for state specific customized items charged to the state requesting those items per the same forty (40) hours rule.
    - iii. Other Consortium Members may, at their sole discretion, establish their own Service cost and approval policies. These thresholds may include but are not limited to SOW costing versus T&M costing, or that any or all work will be performed solely under T&M costing or SOW costing.

#### **D. CORE Perfective Maintenance Service Requirements Processes**

111. The Vendor should expect one of two processes for work that has been determined to be CORE for requirements gathering.
- a. Initial requirements may be gathered by one member state. If the second state approves the project, each state has the option to add additional state specific requirements. The Vendor shall split the initial cost of the project over the

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- participating Consortium states and cost any state specific items directly to the state requesting non-CORE items.
- b. Requirements are gathered collaboratively. In these cases, the states work together to develop CORE and state specific items that are relayed to the Vendor after completion of the requirements. The Vendor then has an opportunity to ask questions and make suggestions with all the participating states at one time. The Vendor shall split the cost of the project over the participating Consortium states and cost any state specific items directly to the state requesting non-CORE items.
- c. For CORE projects, the Vendor will communicate with assigned staff, typically a Business Analyst (BA), from the initiating state who will coordinate any meetings, questions, reviews, and needed decisions. Any necessary signatures will be from the Executive Level Signatory of each state or his/her designee.
- d. Each Consortium member shall set the parameters for any custom projects.

#### **IX. MAINTENANCE AND SUPPORT**

##### **A. Maintenance and Support Services**

- 112. As noted, the Standard Contract described in Exhibit A to this RFP, the State owns the code that the Vendor shall maintain, support, and provide adaptive maintenance for said code. As such, the Vendor shall support all of the code of any type that comprises the ReEmployUSA system without regard to the vendor that created it.
- 113. Management of the work to maintain capacity employing the support levels described to prioritize the work:
  - a. High Priority work will consist of 20% of the workload.
  - b. Medium Priority work will consist of 50% of the workload.
  - c. Low Priority work will consist of 30% of the workload.
- 114. Historical volume of work is presented below to assist in the preparation of RFP responses. Current work, whether production support services or corrective maintenance services, include the following monthly volume that is anticipated to be between 100 and 200 items for MDES and between 200 and 300 for the MDOL.

##### **B. Production Support Services Disaster Recovery:**

###### **i. Security Monitoring**

- 115. Provide Emergency support services 24x7 for the duration of a declared emergency or disaster as determined by the State(s).
- 116. May require immediate dispatch of Vendor's Help Desk staff during some emergencies or disasters. Shifts are typically 8:00 a.m. to 8:00 p.m. and during an emergency, 8:00 p.m. to 8:00 a.m. Failure to have appropriate response times from the Vendor's Help Desk may result in a penalty assessment. See Table 6 Disaster Recovery Maximum Penalties, SLA-003.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

117. As part of these requirements under this RFP, if the Vendor is not in complete control of software license, subscription, or infrastructure, the Vendor will assist with the disaster recovery plan to the maximum extent of the resources it controls.
118. Baseline Update for the ReEmployUSA Disaster Recovery Plan, including the following:
  - a. Supporting information including Business Impact Analysis, Point of Contact Lists, and Roles and Responsibilities.
  - b. Activation, notification, and outage assessment.
  - c. Recovery, sequence of services, and escalation.
  - d. Reconstitution, concurrent processing, data and functionality validation, notifications, cleanup, backup, and event documentation.
  - e. Appendices with any needed details.
  - f. Semi-annual Updated Disaster Recovery Plan. Failure to provide an updated disaster recovery plan may result in a penalty assessment. See Table 6 Disaster Recovery Maximum Penalties, SLA-012.
119. The Vendor will provide proof of disaster recovery readiness immediately upon request by a Consortium Member State(s) or the PMO.
120. The Vendor will provide *After Action Reports* following any disaster recovery exercises, tests, or actual incidents Failure to timely provide After Action Reports may result in a penalty assessment. See Table 8 Disaster Recovery Maximum Penalties, SLA-DR04e Monitoring:
  - i. Performance Monitoring**
    121. The Vendor will set up logs, metrics, and auditing for a monitoring and alerting strategy.
    122. The Vendor will provide regular performance tuning on a monthly basis. Failure to timely perform monthly performance tuning may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-002.
    123. The Vendor will implement a system for collecting and addressing user feedback.
    124. The Vendor will ensure that AI/BOT/System failures are reported to the Consortium members immediately.
  - ii. Security Monitoring**
    125. The Vendor will work with MDES/Consortium States internal teams to ensure that security is considered at all phases. The Vendor will proactively analyze, detect, and prevent threats to the system utilizing MDES/Consortium States approved tools, processes, and procedures and testing procedures including penetration testing. When threats are uncovered, the Vendor will contain, mitigate, and resolve threats or security issues.
      - a. The Vendor will retain and use in-house expertise to ensure the Information Data Security Plan aligns with industry standards.
      - b. The Vendor will execute security procedures in accordance with the approved Information Data Security Plan.



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

#### iii. Corrective Maintenance Services

126. The Vendor's responsibility is to limit the threshold for Vendor defects to less than five percent (5%) of overall monthly work items. Remediation under the Vendor's maintenance and support responsibilities shall include all Vendor-generated defects including those above five percent (5%) of the overall monthly work items. Each Consortium State, at its discretion, may negotiate a different level for either or both Vendor defects and Vendor responsibility as it deems appropriate.
127. Corrective Maintenance Services related to new perfective maintenance services will be covered under the standard corrective maintenance services of this RFP no matter if the perfective maintenance Service was developed under T&M, a SOW, a CO-SOW, or by a different vendor.

#### v. Adaptive Maintenance Services

128. While the Vendor may not be the lead on all upgrades, the Vendor is required to assist as required in any upgrade.
129. The Vendor will identify each vulnerability as Critical, High, Medium, or Low. Based on the level of each vulnerability the patching requirements are:
  - a. Critical Vulnerabilities – remediated within 14 days
  - b. High Vulnerabilities – remediated within 30 days
  - c. Medium Vulnerabilities – remediated within 60 days
  - d. Low Vulnerabilities – remediated within 90 days.

Failure to identify each vulnerability and meet the remediation requirements under SLA-015 may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-015.

130. The Vendor will provide a monthly report showing all identified vulnerabilities, all patched vulnerabilities, and the vulnerability patching rate. Each identified vulnerability will show the level of vulnerability as Critical, High, Medium, or Low. Failure to timely deliver the report may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
131. In the event that the update to CORE is required because of a failure of the Vendor to appropriately and promptly perform patches or minor upgrades, either critical or routine, or any previous updates to the CORE, then the Vendor will bear responsibility for any costs related to its failure including but not limited to major upgrades.
132. The Consortium States anticipate that the Vendor will perform patching per SLA-014, or for critical security vulnerability patches immediately after notification to the appropriate Consortium States so as to always maintain a stable and secure system. Failure to perform timely patching may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-014.
133. The Vendor shall not fall behind or impede the timely implementation of system patches and minor upgrades, both routine and critical, or otherwise jeopardize the security of the system.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

#### vi. Preventive Maintenance & Performance Management Services

134. The Vendor shall perform performance management for development services included in the list below. System performance will be monitored through the metrics outlined in *Appendix D - Software Development Performance Monitoring*. Performance metrics will be compiled by the PMO and provided to the Vendor. Failure to meet performance management requirements may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-002.
  - a. Surveys - Surveys will help the Consortium States focus on end-user support and satisfaction to address reliability, usability, and Vendor performance and satisfaction.
  - b. Time to Production - A measure that displays how fast the Vendor delivers on the required items and user stories. This metric will determine if each Consortium State gained the appropriate value proposition and receives the right product at the right cost.
  - c. Cost - In an effort to encourage the Vendor to optimize the size of each team, each Consortium States will measure the ratio of the cost of the sprint over the number to story points completed in a sprint.
  - d. Code Quality - Each Consortium State will monitor code quality through in-house processes and software tools such as SonarQube. Each Consortium State and the Vendor will collaborate on the acceptable metrics for code quality during the first ninety (90) days after the contract start date.
135. Additional performance management requirements for development services will be included in SLAs and KPIs, to be defined by the Consortium States.

#### X. ADMINISTRATION

##### A. Billing Practices

136. The Vendor will provide the following types of invoices plus any other invoices deemed necessary and as agreed upon by the Consortium state(s) or a billing plan that demonstrates alternative billing practices that provides this same information in an alternative manner. The Consortium States, at their sole discretion, have the right to refuse this billing plan and require the billing practices as laid out below.
  - a. Monthly Maintenance and Support – The Vendor will include the following, on, or as an attachment to, all monthly fixed cost Maintenance and Support invoices:
    - i. The identification number used in the Consortium States' ticketing system.
    - ii. A summary of the item being billed.
    - iii. Completion percentage of the item.
  - b. Individual State T&M – The Vendor will include the following on or as an attachment to all T&M invoices:
    - i. The identification number used in the Consortium States' ticketing system of each item.
    - ii. A summary of the item being billed.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- iii. The Vendor staff who worked on the item.
  - iv. The number of hours the Vendor staff worked on the item by staff member.
  - v. Completion percentage of this item. If the completion percentage is 100%, the Vendor must attach the report outlined above in the Product Release Process. Failure to provide the required documentation with invoices may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
  - vi. In states where T&M projects require pre-approval, the Vendor will also provide the estimated costs that were approved and the approver.
  - vii. For any invoice that has the completion of a product, the Vendor shall include the final project report. See SLA-012 and Section IV(B) for further information.
- c. Shared Projects (includes T&Ms and SOWs), and Shared Services (T&Ms) – The Vendor will send a copy of this invoice to all participating Consortium States showing the total and individual costs for all shared projects or projects using shared services and will include the following information:
- i. The identification number used in the Consortium States' ticketing system of each item.
  - ii. A summary of the item being billed.
  - iii. The Vendor staff who worked on the item by Consortium State.
  - iv. The number of hours the Vendor staff worked on the item by staff member and by Consortium State.
  - v. Completion percentage of this item by Consortium State. If the completion percentage is 100%, the Vendor must attach the report outlined above in the Product Release Process. Failure to provide the required documentation with invoices may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
  - vi. In states where T&M services require preapproval, the Vendor will also provide the estimated costs that were approved and the approver.
  - vii. For any invoice that has the completion of a product, the Vendor shall include the final project report. See SLA-012 and Section IV(B) for further information.
- d. SOW Milestone and CO-SOW Milestone – The Vendor will include the following as an attachment to all SOW Milestone invoices or CO-SOW Milestone invoices:
- i. Completion percentage of this project by Consortium State & a brief Progress Report for any corrective, adaptive, or perfective maintenance services listing status of the Service, the number of professional service hours expended, and the percentage of the work completed.
  - ii. Documentation showing completion of the milestone.
  - iii. For the final milestone, the Vendor shall include the final product report. See SLA-012 and Section IV(B) for further information.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

137. The Vendor is encouraged to present alternative pricing models that may yield greater cost savings for this RFP. For *Attachment C - Cost Information Submission Form* the Vendor will provide a fixed cost price for maintenance and support work including but not limited to Sections IX below.
138. The Vendor agrees to alter billing practices as required by the Consortium State(s) to arrive at a billing process conducive to the verification of the work performed for the Consortium States.
139. The Consortium States understand that the fixed price for maintenance and support will be presented per year in this RFP and on *Attachment C - Cost Information Submission Form*.
140. All T&M items will be billed using the Fully-loaded Hourly Time and Materials Rate provided in *Attachment C - Cost Information Submission Form*.
141. All SOWs will be prepared using the Fully-loaded Hourly Perfective Maintenance Service Statement of Work Rate provided in *Attachment C - Cost Information Submission Form*.
142. All CO-SOWs will be prepared using the Fully-loaded Hourly Change Order Rate provided in *Attachment C - Cost Information Submission Form*.

#### B. Vendor Capacity

143. Vendor Capacity:
  - a. The Vendor must manage their capacity in order to maintain the workloads described in paragraph 110 above.
  - b. The Vendor must provide a human resources allocation report monthly to each individual Consortium State for their assigned staff, and
  - c. The Vendor must provide a human resources allocation report for shared resources to all Consortium states.
  - d. These reports should, for the prior month, list all assigned employees or subcontractors, their assigned projects, employee location, pending Visa issues (if any), time-off requests that exceed one week, position, and the number of hours actually worked by each employee or subcontractor on each project.
  - e. This report should be presented to the individual Consortium states by the 15<sup>th</sup> day of the following month. Failure to timely deliver monthly human resource allocation reports may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
144. Audit Assistance
  - a. The Vendor will be required to assist Consortium States with federal and state audits, Vendor certifications, and other audits as the Consortium States deem necessary.
  - b. Required Audits
    - i. State Auditor
    - ii. Department of Labor (DOL) and any departments therein

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

- iii. Internal Revenue Service
- iv. Social Security Administration
- c. The Vendor is required to comply with all audits as specified by Consortium States.
- d. The Vendor will provide full support of audits of the ReEmployUSA system along with any related systems, software, services, and tools.
- e. The Vendor will utilize Time & Materials costing for tasks related to completion of the Audit outside of those tasks listed as Production Support Services.
- f. Costs of Remediation of problems/issues found during the audit(s) are the responsibility of the Vendor unless one of the following three (3) items is true as determined by the individual Consortium State or States.
  - i. The Consortium State(s) independently procured tools, services, hardware, or software failed to meet specifications required for the audit
  - ii. The issues identified in the audit are already planned for remediation as part of an existing or planned perfective maintenance Service.
  - iii. The audit finding resulted from the Consortium State(s) interpretation and/or direction that can be shown through documentation.
- g. The Vendor will timely resolve findings related to audits after working with the State(s) to determine appropriate response.

#### **XI. PRODUCTION SERVICE LEVEL AGREEMENTS (SLAs) AND KEY PERFORMANCE INDICATORS (KPIs)**

##### **A. KPI/SLA's**

- 145. The Consortium States have identified specific KPIs to be key indicators of the UI System's operational performance and of the Vendor's support. The Vendor shall bear responsibility for the management of the system. Penalties described in this RFP for failure to meet an SLA or KPI may be assessed after documentation by any affected Consortium State independently.
- 146. KPIs/SLAs will be agreed upon by the Vendor and the Consortium. Additional KPIs/SLAs may be added by the Consortium. Table 5 provides the KPIs and SLA's.

**Table 5 - KPIs/SLAs**

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
SLA-001	System Uptime	<p>System availability is defined as the percentage of possible uptime in a month that the production environments supporting the Consortium Unemployment Systems (including all associated components implemented and controlled by the Vendor) are available to users, to perform back-end processing, or to perform in a back-up capacity. Negotiated downtime for system maintenance during off-peak hours (7:00pm to 7:00am), where the time zone is relative to the Consortium State, is not included in the calculation of system availability.</p> <p><b>Downtime Defined</b> Downtime is defined as the time during which any component(s) of the system is not functioning or available for any reason. Production downtime is the time during which the system is not available for its intended use in production. There are two types of downtime, as defined below:</p> <ol style="list-style-type: none"> <li>1. <u>Scheduled Downtime</u>: Any period of time that the system, or any component(s) of the system, is unavailable for its intended use that has been reviewed and approved by Consortium in advance of the service interruption. Scheduled downtime, that has received approval from a Consortium member, does not count towards downtime performance standards.</li> <li>2. <u>Unscheduled Downtime</u>: Any period of time that the system, or any component(s) of the system, is unavailable for its intended use that has not been approved by Consortium in advance of the service interruption.</li> </ol> <p>Unscheduled downtime may occur as a result of various issues, outside of the Vendor’s control and not pertaining directly and solely to problems associated with the baseline Unemployment Systems. The Vendor must email the group identified by the affected Consortium State(s) with the downtime reason within fifteen (15) minutes of discovery.</p> <p>For any downtime, the Consortium UI System must automatically re-connect to all interfaces and external integration points and deplete all externally queued or backlogged files and transactions within twenty-four (24) hours of System operational resumption</p> <p>The Vendor must ensure that all Robotic Processing Automation (RPA) BOTS, AI, or other automated features in the system are operating as expected. The Vendor must email the group identified by the affected Consortium State(s) with the downtime reason within fifteen (15) minutes of discovery.</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p><b>Performance Standard</b></p> <p>The Vendor must ensure system availability of 99.99% during peak hours (7:00 am to 7:00 pm Monday-Friday) based on applicable time zone and of 99.9% during off-peak hours (7:00 pm to 7:00 am Monday-Friday and Saturday-Sunday), as it pertains directly and solely to availability of the baseline UI Systems.</p> <p>The Vendor must report any BOT failure, delay in scheduled processing, AI failure, or any other item affecting the proper functioning of the RPA BOTS or AI within fifteen (15) minutes of discovery. See SLA-012 for reporting requirements.</p>
<b>SLA-002</b>	System Performance and Performance Monitoring	<p>System performance is defined as the time it takes for the system to complete actions initiated by a system user.</p> <p><b>Performance Standards</b></p> <p>The Vendor must ensure a system performance response time of less than or equal to two (2) seconds for the following:</p> <ul style="list-style-type: none"> <li>• Menus within the Baseline Application</li> <li>• Query to and from Database via Baseline Application</li> <li>• Web-Enabled Programs</li> <li>• Application pages are to be submitted, processed, and returned back to the user while the system is under peak loads.</li> </ul> <p>An average time will be computed from five (5) consecutive system transactions at random times and with the transaction type(s) selected by the Consortium.</p> <p>The Vendor will establish logs, metrics, and auditing for a monitoring and alerting strategy for performance monitoring per the metrics outlined in Appendix D - Software Development Performance Monitoring.</p> <p>The Vendor will perform monthly performance tuning.</p> <p>The Vendor will implement a system for collecting and addressing user feedback.</p> <p>After the Vendor has completed six (6) sprints, the Consortium in conjunction with the Vendor shall establish baselines and required reporting frequency for all of the following Performance Monitoring items. The Vendor will provide documentation to show that they are meeting or exceeding the agreed upon baselines at the reporting frequencies established. Appendix D - <i>Software Development Performance Monitoring</i> of this RFP provides additional technical information for this SLA.</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<ul style="list-style-type: none"> <li>• Defect Density</li> <li>• Defect Detection Percentage</li> <li>• Escape Rate</li> <li>• Cyclomatic Complexity</li> <li>• CORE Code Coverage</li> <li>• Code Quantity</li> <li>• Cycle Time</li> <li>• Lead Time</li> <li>• Velocity</li> <li>• Code Churn</li> <li>• Sprint Burndown</li> </ul> <p>The Vendor will conduct performance management for development services including surveys, time to production, cost and code quality per the metrics outlined in Appendix D - <i>Software Development Performance Monitoring</i>.</p>
<b>SLA-003</b>	Technical Support	<p>The Vendor must provide technical support for Consortium users who report technical problems, assist with problem analysis, and provide support to the Consortium for troubleshooting problems, where that support is consistent with the terms of this SLA and any future mutually agreed to support agreements.</p> <p><b>Tracking of Support Inquiries</b> The Vendor shall maintain sufficient staff and systems to manage, track, and report on technical support services via multiple channels, including telephone, client portal, email, and mail.</p> <p><b>Hours of Operation</b> Consortium User Technical Support Standard Hours of Operation are 8 a.m. through the completion of all daily batches in addition to sprints and other specialized circumstances as defined by the state.</p> <p>Standard Disaster or Emergency Hours of Operation are 24 hours a day, 7 days per week.</p> <p><b>Performance Standards</b> The Vendor will ensure user support meets the following performance standards:</p> <p><b>Average Speed of Answer.</b> It is expected that the Vendor’s staff will respond to inquiries during the standard hours of operation listed above within thirty (30) minutes. This standard will be considered met so long as the Consortium State leaves a message (by phone or email) with the Vendor, and the Vendor</p>



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>responds to the message and connects directly with Consortium staff within forty-five (45) minutes.</p> <p>For disasters or Emergencies identified outside of the standard hours of operation, it is expected that the Vendor’s staff will respond to inquiries within one hour.</p>
<b>SLA-004</b>	Data Recovery	<p>Data Recovery is defined as retrieving inaccessible, lost, corrupted, damaged, or formatted data from the data repository(s).</p> <p><b>Vendor Control</b> No data loss except for data collected after the last committed transaction.</p> <p><b>Performance Standards</b> Excluding disaster recovery scenarios, see DR SLAs for more information regarding DR data recovery requirements, there shall be no data loss experienced by the Consortium member State(s). The Consortium State(s) will utilize queries of the data repository(s) to ensure compliance.</p>
<b>SLA-005</b>	Peak Expansion/Growth Factor	<p>Peak Expansion/Growth Factor is defined as the storage capacity and ability to expand system capabilities due to changes in business requirements, legislation changes and/or modernization.</p> <p><b>Performance Standards</b> The Vendor will maintain sufficient resources to expand system capabilities as required because of business requirements, legislation changes, modernization, U.S. Department of Labor UIPLs and/or other Federal Legislative changes based on changing priorities.</p>
<b>SLA-006</b>	Support Service Issue Management	<p>The Vendor is to provide support Service issue management and resolve problems with the enterprise solution consistent with the terms of the RFP. Issues identified are to be categorized based upon severity, communicated to the Consortium State(s), documented, resolved, and tracked by the Vendor in a form and format accessible to, and approved by the Consortium.</p> <p><b>Issue Tracking</b> A Consortium approved tool will be used for the tracking of defects from identification through resolution (during UAT as well), including all testing performed to ensure the correct fix is in place. Currently this tool is Jazz, and we are migrating to Jira. This tool may change according to the needs of the Consortium State(s).</p> <p><b>Performance Standards</b></p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>The Consortium State(s) and the Vendor shall categorize/set the priority for each issue, and the Vendor shall resolve all errors in accordance with the following:</p> <p>The Vendor is expected to resolve issues based on the categorization/priority set by each state.</p> <ol style="list-style-type: none"> <li>a. Critical Issue – Immediate remediation until deployed. Patched if possible.</li> <li>b. High Priority Issue – Remediation within 1 week or other such time as agreed upon with each Consortium State.</li> <li>c. Medium Priority Issue – Remediation by next build.</li> <li>d. Low Priority Issue – Remediation by next build.</li> </ol> <p>The Vendor’s responsibility is to limit defects to less than five percent (5%) of overall monthly maintenance and support items.</p>
<b>SLA-007</b>	Regular Operational Reporting	<p><b>Performance Standards</b> The Vendor will ensure production operational reporting meets the following performance standards:</p> <p>Note that these performance standards and penalties apply to the extent the accepted production operational reports are unavailable due to an issue solely within the baseline Unemployment Systems application.</p> <p><u>Reports Availability Schedule:</u> Reports should be aggregated by process areas and functionalities.</p> <ul style="list-style-type: none"> <li>• Daily Reports: Beginning of the following business day.</li> <li>• <u>Monthly Reports:</u> Beginning of the following <u>business day following the end of the month.</u></li> <li>• <u>Quarterly Reports:</u> Beginning of the following <u>business day following the end of the quarter.</u></li> <li>• <u>Annual Reports:</u> Beginning of the following <u>business day following the end of the annual period (Calendar or fiscal).</u></li> </ul>
<b>SLA-008</b>	System Security and Security Monitoring	<p>See the following: Information Data Security Plan, IRS Publication 1075, OF-4 Requirements Traceability Matrix, System and Security tabs, NIST 800-53 Rev. 5, SSA requirements, 20 C.F.R. Section 603, CISA Cybersecurity best practices, SOCM Audit requirements, all Federal Tax Information (FTI) requirements, and individual Consortium State’s Information Technology Agency requirements.</p> <p><b>Performance Standards</b> The Vendor must maintain compliance with the above-listed security requirements, audits, matrices, publications, and best</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>practices. When the Vendor becomes aware that, or is notified by, a Consortium state of non-compliance in any of the above listed items, the Vendor must prepare a security remediation plan with the information listed below and present it to the Consortium Technology Committee within five (5) business days. The Technology Committee, or the individual State’s representative to that Committee, will review the Vendor’s report as defined below to determine if acceptable or identify changes that must be made. The Vendor must present all of the following as part of the remediation plan:</p> <ul style="list-style-type: none"> <li>• An explanation and documentation, if available, for security non-compliance</li> <li>• Interim mitigation actions to overcome the non-compliance.</li> <li>• Expected timeline to complete the remediation.</li> </ul> <p>The Vendor will execute security procedures in accordance with the approved Information Data Security Plan.</p>
<b>SLA-009</b>	Sensitive Data, Cyber Attack, Cyber Security Incident, Breach, and Data Breach	<p><b>Performance Standards</b></p> <p>The Vendor will provide initial notice of any Cyber Attack, Cyber Security Incident, Breach, or Data Breach to the Consortium within Thirty (30) minutes of the Vendor’s identification of the potential issue. The Vendor will then provide periodic updates as to the status of the incident, after action reports, etc.</p> <p>Cyber Attacks, Breaches, and Data Breaches are considered Critical Issues with the associated resolution timelines.</p>
<b>SLA-010</b>	Vendor Cooperation with Infrastructure Services Vendor	<p>In all cases including an incident or breach, that is determined to not be directly related to the application, the Vendor will work with other teams, including the infrastructure team, to the maximum extent required to ensure that all KPIs are met.</p> <p><b>Performance Standard</b></p> <p>The Vendor will provide timely responses and staff availability as needed to the infrastructure services Vendor and be available as needed to complete Infrastructure Services projects. Delays in Infrastructure Services work where documentation exists showing the delay is due to the poor responsiveness or unavailability of this Vendor’s staff will result in penalties. The Consortium member shall have the right to document State expenses due to these delays and the Vendor will be responsible for these costs.</p>
<b>SLA-011</b>	Staffing and Key Resources	<p><b>Performance Standards</b></p> <p>The Vendor will maintain staffing levels defined in the resulting Agreement. Vacancies due to the departure of key positions must be communicated to the appropriate Consortium State within three (3) business days of the staff’s departure.</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>Replacements of key resources will be communicated to the Consortium State within five (5) business days of the hiring of a new key resource. If there is a turnover of 3 or more key positions in in any three (3) month period, the affected Consortium member shall have the right to secure its own contract staff at the Vendor's expense.</p> <p>Holidays - The Vendor must advise MDES / Consortium State(s) of any holidays (e.g., religious, cultural, etc.) other than State holidays that may result in the absence of three (3) or more employees, subcontractors or any key position. The Vendor must send notice fourteen (14) days in advance of any such holidays and must include the names of affected employees, subcontractors, or any key position.</p> <p>Vacations - The Vendor shall notify MDES / Consortium State(s) at least fourteen (14) business days prior to any employee's or subcontractor's scheduled vacation with a duration of more than five (5) business days.</p>
SLA-012	Required periodical testing and reporting	<p>Periodical testing, updates, and reports must be reported as defined below.</p> <p><b>Performance Standards</b> <b>Monthly:</b></p> <p>The Vendor must provide a human resources allocation report monthly to the PMO and each individual Consortium State for their assigned staff and to the PMO and all Consortium States for their shared resources, for the prior month. These reports must list all assigned employees or subcontractors, their assigned projects, employee location, pending Visa issues (if any), time-off requests that exceed one week, position, and the number of hours actually worked by each employee or subcontractor on each project. This report will be provided to States by the 15<sup>th</sup> day of the month following the reported month.</p> <p>The Vendor will provide, as a part of the product release requirements, a monthly report showing the manual and automated test coverage percentage, number of manual &amp; automated test cases performed, and total number of test cases performed for each product in system testing during that month.</p> <p>The Vendor will provide a monthly report showing all identified vulnerabilities, all patched vulnerabilities, and the vulnerability patching rate. Each identified vulnerability will show the level of vulnerability as Critical, High, Medium, or Low.</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>The Vendor will generate a monthly performance report card for each state on all KPIs, regarding the prior month’s performance. The Vendor shall ensure that all data and data elements necessary to support agreed upon SLAs and metrics will be collected and measured and can be monitored by the Consortium States. The monthly performance report card for a completed month will be provided to each Consortium state within five (5) business days of the 1<sup>st</sup> of each month.</p> <p><b>Quarterly:</b>  SLA Review - The successful Vendor shall work with the Consortium to continually refine the data to be used, calculations, and monitoring approach for all aspects of all agreed upon SLAs and metrics for the first year of this contract.</p> <p><b>Semi-annually (180 days):</b>  The Vendor will review, update, and deliver the “technical roadmap” every 180 days to ensure consistency with current technologies and notify each Consortium member state of all changes when implemented.</p> <p>The Vendor will review, update, and deliver the “business roadmap” every 180 days to ensure consistency with current technologies and notify each Consortium member state of all changes when implemented.</p> <p>The Vendor will update and provide recommendations to the Cyber Security Risk Mitigation plan and provide to the Consortium States for approval every 180 days. The plan will include all tools software, and security mechanisms currently utilized by the Consortium States.</p> <p>The Vendor will provide an updated Disaster Recovery Plan.</p> <p><b>Annually:</b>  The Vendor will perform Failover testing and Failback testing no less than every 365 days with testing criteria that are pre-approved by each Consortium State or the Consortium PMO.</p> <p>The Vendor will provide compliance documentation annually or upon request by a Consortium State that the system is in compliance with IRS publication 1075, NIST 800-53 Rev 5, SSA requirements, OF-4 requirements, and 20 C.F.R Section 603 or any update, revision, or future security compliance as required by the Consortium State(s).</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>The successful Vendor shall work with the Consortium to continually refine the data to be used, calculations, and monitoring approach for all aspects of all agreed upon SLAs and metrics for years two (2) through five (5) of this contract and any extensions or amendments.</p> <p><b>Within a specified Timeframe of an event:</b>                      The Vendor will update the Information Data Security Plan within 30 days of a change, alert, or release of guidance by the IRS, SSA, NIST, or an individual state(s) Information Technology Agency.</p> <p>The Vendor will submit a written CAP for approval by the requesting Consortium State(s) no later than ten (10) business days from the date of the CAP request.</p> <p>The Vendor will provide After-Action Reports following any RPA BOT or AI incident within 10 days of the event.</p> <p>The Vendor, as a part of the product release requirements, will provide a report for each product at the conclusion of system testing showing the manual and automated test coverage percentage, number of manual and automated test cases performed, and total number of test cases performed during system testing for that product.</p> <p>The Vendor, as a part of the product release requirements, will provide a report as outlined in the Product Release Requirements section of this document.</p>
SLA-013	Billing and Invoicing	<p>The Vendor is to provide separate Consortium state billing and invoicing in a way that allows the States to easily identify work that has been completed, which Vendor staff completed the work, the completion percentage of the items, and verify those to ensure that funds are utilized in the best interest of the individual state. The Consortium states must also be able to easily identify shared services and projects and how these are being billed across all participating states.</p> <p><b>Performance Standards</b>                      See Section X(A) for details of what items are required to be included in each invoice type listed.</p> <p>The Vendor will produce monthly Maintenance and Support invoices.</p> <p>The Vendor will produce monthly Individual State T&amp;M invoices.</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>The Vendor will produce monthly Shared Services invoices.</p> <p>The Vendor will produce monthly Share Projects invoices (Both T&amp;M and SOWs).</p> <p>The Vendor will produce SOW Milestone invoices.</p> <p>The Vendor will produce invoices that have all the required documentation and supporting documentation in one file with all documentation. For MDES this shall be one single PDF per invoice. Other Consortium states may establish their invoicing requirements.</p>
<b>SLA-014</b>	Maintenance and Support Services	The Vendor will perform all Maintenance and Support as defined in this RFP under the monthly fixed cost price established under the contract.
<b>SLA-015</b>	Vulnerability Patching Rate	<p><b>Performance Standards</b></p> <p>Each identified vulnerability will have an identified level of vulnerability as Critical, High, Medium, or Low.</p> <p>For any vulnerability that cannot be remediated within the listed timeframes, the Vendor must notify the Consortium Technology Committee as soon as the inability to timely remediate is known. The Technology Committee, or the individual State’s representative to that Committee, will review the information presented below to determine if the failure to timely remediate is allowable or should result in penalties. The Vendor must present the following:</p> <ul style="list-style-type: none"> <li>• An explanation and documentation if available for the inability to patch in a timely manner.</li> <li>• Interim mitigation actions to overcome the failure to patch in a timely manner.</li> <li>• Expected timeline to complete the remediation.</li> </ul>
<b>SLA-016</b>	Product Release Requirements	<p><b>Performance Standards</b></p> <p>The Vendor will perform a Change Impact Analysis.</p> <p>The Vendor will provide system use cases (SUCs) to the Consortium State(s).</p> <p>The Vendor will perform System Testing and provide the Consortium State(s) with detailed results of said testing.</p> <p>The Vendor will conduct a product demonstration of all new products prior to releasing the product to user acceptance testing.</p> <p>The Vendor will release the product into User Acceptance Testing a minimum of fourteen (14) days before a production release to</p>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	SLA Description
		<p>ensure time for Consortium State(s) to adequately perform user acceptance testing.</p> <p>The Vendor shall not release a product to production without the Consortium State(s) official approval. This approval requires completion of a product demonstration and completed user acceptance testing.</p> <p>The Vendor will create or update user manuals for changes made to the system including but not limited to screen changes, functionality changes, or role/access changes.</p>
<b>SLA-017</b>	CAP Failure	<p><b>Performance Metrics:</b> The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 3 failures of the same SLA within a 12-month period.</p>

#### B. KPI Failure and Maximum Penalties

147. KPI Failure - In the event specific KPIs are not met, the applicable Consortium State, after documenting such failure, will follow the below guidelines.

- a. Right to Payment Reduction- If an individual state demonstrates a KPI failure and elects to impose a penalty, as listed in Table 6, the penalty amount will be deducted from the next monthly Maintenance and Support invoice for that individual state.

SLA-001's and SLA-003's penalties may be assessed on a daily basis up to the maximum penalty. SLA-002 and SLA-004 through SLA-017's penalties may be assessed on a monthly basis up to the maximum penalty. See Table 6 for the Maximum Penalties.

- b. Maximum Payment Reduction Percentages - The maximum fees assessed by any Consortium State must not exceed 100% of that state's monthly allocation of the annual UI Systems Maintenance and Support fees per Consortium State.
- c. In the event that the maximum payment reduction fees assessed equal or exceed 100% for any consecutive 2-month period, the Vendor may be deemed to be in breach of the Contract and may be subject to Termination at the discretion of the individual Consortium States. Cybersecurity incident zero payment under 136(d)(1) will only be counted as 1 month per event for purposes of this subsection.
- d. **MANDATORY:** Sensitive Data, Cyber Attack(s), Cyber Security Incident(s), Breaches, or Data Breaches – All items under this paragraph are mandatory.
  - i. Zero Payment –
    - a. In the instance of a Cyber Attack, Breach, or Data Breach, each affected Consortium State(s), shall reduce its monthly payment for a six (6) month period from the event date. This reduction may



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

- occur in addition to any other rights available to each affected Consortium State.
- b. In the event of more than one (1) Cyber Attack, Breach, or Data Breach within a six (6) month period, the Consortium State(s) may increase the duration of the zero-payment period to include a full six (6) month period per event, or deem the Vendor to be in breach of the Contract and may subject the Vendor to Termination at the sole discretion of the affected Consortium State(s).
  - ii. Credit Monitoring - In the instance of a Cyber Attack, Breach, or Data Breach, all affected Consortium States, shall have the right to require the Vendor to provide Free Credit Monitoring and identity theft protection for three (3) years to all affected customers from the date of the attack or breach. This right is in addition to any other rights available to each affected Consortium State. Each Attack or Breach shall require a separate three (3) year Free Credit Monitoring and identity theft protection package.
  - e. Monthly Reporting - A performance report card for each state will be generated monthly on all KPIs defined herein, regarding the prior month's performance. The successful Vendor shall ensure that all data and data elements necessary to support agreed upon SLAs and metrics will be collected and measured and can be monitored by the Consortium States. All reports and data used in the determination of SLA compliance and calculation of KPI metrics shall be made available to the Vendor by the Consortium. Failure to provide the required monthly reporting may result in a penalty assessment. See Table 6 Maximum Penalties, SLA-012.
  - f. SLA Review - The successful Vendor shall work with the Consortium to continually refine the data to be used, calculations, and monitoring approach for all aspects of all agreed upon SLAs and metrics. The Vendor and the Consortium will jointly review all KPIs and Performance Measures to determine if measures require revision. Thereafter, similar reviews shall occur upon all of the following events. See SLA-012 for more information.
    - i. Quarterly Review for the first year, annually thereafter.
    - ii. Material changes to the maintenance and support services that impact existing KPIs. and
    - iii. Upon the request of any Consortium member.

**Table 6 - Maximum Penalties**

KPI Identifier	KPI Name	Maximum Payment Percentage Reduction Per Month
SLA-001	System Uptime	20.0%
SLA-002	System Performance and Performance Monitoring	20.0%
SLA-003	Technical Support	20.0%
SLA-004	Data Recovery	20.0%
SLA-005	Peak Expansion/Growth Factor	20.0%
SLA-006	Support Issue Management	20.0%

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

KPI Identifier	KPI Name	Maximum Payment Percentage Reduction Per Month
SLA-007	Regular Operational Reporting	20.0%
SLA-008	System Security and Security Monitoring	20.0%
SLA-009	Sensitive Data, Cyber Attack, Cyber Security Incident, Breach, and Data Breach	100.0%
SLA-010	Vendor Cooperation with Other Vendors	20.0%
SLA-011	Staffing and Key Resources	20.0%
SLA-012	Required periodical testing and reporting	20.0%
SLA-013	Billing and Invoicing	20.0%
SLA-014	Maintenance and Support Services	20.0%
SLA-015	Vulnerability Patching Rate	20.0%
SLA-016	Product Release Requirements	20.0%
SLA-017	CAP Failure	50.0%

#### C. Disaster Recovery SLAs and KPIs

148. Disaster Recovery KPI/SLA Overview - The Consortium States have identified specific disaster recovery KPIs to be key indicators of the Disaster Recovery performance of the Vendor. The Vendor shall bear responsibility for remaining ready for disaster recovery.
149. Disaster Recovery KPIs/SLAs will be agreed upon by the Vendor and the Consortium. Additional KPIs/SLAs may be added by the Consortium. Table 7 provides the Disaster Recovery KPIs and SLA's.

**Table 7 – Disaster Recovery KPIs**

KPI Identifier	KPI Name	SLA Description
SLA-DR01	Recovery Point Objective (RPO)	<b>Performance Standard</b> The Maximum amount of data, measured by time, can be lost after a recovery from a disaster/failure. The maximum time allotted is fifteen (15) minutes.
SLA-DR02	Recovery Time Objective (RTO)	<b>Performance Standard</b> The maximum time to recover a system after an outage or disruption. The maximum time allotted is four (4) hours.
SLA-DR03	Disaster Recovery Readiness	<b>Performance Standard</b> The Vendor will upon request immediately provide documentation of the Disaster Recovery Readiness to each Consortium State and will work with the infrastructure Vendor of each state to ensure Disaster Recovery Environment Readiness.
SLA-DR04	After Action Reports	<b>Performance Standard</b> The Vendor will provide After-Action Reports following any disaster recovery exercise, test, or actual incident.
SLA-DR05	Disaster Recovery Support	<b>Performance Standard</b>

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

		<p>The Vendor will Provide Emergency support services 24x7 for the duration of a disaster or emergency identified by the state.</p> <p>The Vendor must be able to comply with the Consortium State’s or States’ requirement of immediate dispatch of Vendor’s Help Desk staff.</p>
<b>SLA-DR06</b>	Required periodical reporting	<p><b>Performance Standard</b>  <b>Semi-Annually</b>  The Vendor will generate a semi-annual performance report card for each state on all disaster recovery KPIs, regarding the prior six months’ performance. The Vendor shall ensure that all data and data elements necessary to support agreed upon disaster recovery SLAs and metrics will be collected and measured and can be monitored by the Consortium States.</p> <p><b>Annually</b>  The successful Vendor shall work with the Consortium to continually refine the data to be used, calculations, and monitoring approach for all aspects of all agreed upon disaster recovery SLAs and metrics. The Vendor and the Consortium will jointly review all disaster recovery KPIs and Performance Measures to determine if measures require revision.</p> <p><b>Within a specified Timeframe of an event:</b>  The Vendor will submit a written CAP for approval by the requesting Consortium State(s) no later than ten (10) business days from the date of the CAP request.</p>
<b>SLA-DR07</b>	CAP Failure	<p><b>Performance Standard</b>  The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 3 failures of the same SLA-DR within a 12-month period.</p>

#### **D. Disaster Recovery KPI Failure and Maximum Penalties**

150. Disaster Recovery KPI Failure - In the event specific disaster recovery KPIs are not met, the applicable Consortium State, after documenting such failure, will follow the below guidelines.

- a. Right to Payment Reduction- If an individual state demonstrates a Disaster Recovery KPI failure and elects to impose a penalty, as listed in Table 8, the penalty amount will be deducted from the next monthly Maintenance and Support invoice for that individual state.

SLA-DR01’s penalties may be assessed for every 15 minutes that the failure continues up to the maximum penalty. SLA-DR02’s penalties may be assessed for every 4 hours that the failure continues up to the maximum penalty. SLA-DR03’s – SLA-DR07’s penalties may be assessed on a

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

---

monthly basis up to the maximum penalty. See Table 8 for the Disaster Recovery Maximum Penalties.

- b. Maximum Payment Reduction Percentages - The maximum fees assessed by any Consortium State must not exceed 100% of that state's monthly allocation of the annual UI Systems Maintenance and Support fees per Consortium State.
- c. In the event that the maximum payment reduction fees assessed equal or exceed 100% for any consecutive 2-month period, the Vendor may be deemed to be in breach of the Contract and may subject to Termination at the discretion of the individual Consortium States.
- d. Semi-annual Reporting - A performance report card for each state will be generated semi-annually on all disaster recovery KPIs defined herein, regarding the prior six months' performance. The successful Vendor shall ensure that all data and data elements necessary to support agreed upon disaster recovery SLAs and metrics will be collected and measured and can be monitored by the Consortium States. All reports and data used in the determination of disaster recovery SLA compliance and calculation of disaster recovery KPI metrics shall be made available to the Vendor by the Consortium. Failure to provide the required semi-annual reporting may result in a penalty assessment. See Table 8 Disaster Recovery Maximum Penalties, SLA-DR06.
- e. The successful Vendor shall work with the Consortium to continually refine the data to be used, calculations, and monitoring approach for all aspects of all agreed upon Disaster Recovery SLAs and metrics. The Vendor and the Consortium will jointly review all Disaster Recovery KPIs and Performance Measures to determine if measures require revision. Thereafter, similar reviews shall occur as listed below. See Table 8 Disaster Recovery Maximum Penalties, SLA-DR06.
  - i. Annually
  - ii. Material changes to the maintenance and support services that impact existing KPIs. and
  - iii. Upon the request of any Consortium state.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

**Table 8 – Disaster Recovery Maximum Penalties**

Disaster Recovery KPI Identifier	Disaster Recovery KPI Name	Payment Percentage Reduction (SLA-DR01 and SLA-DR02) or Maximum Payment Percentage Reduction (All other SLA-DRs)
SLA-DR01	Recovery Point Objective (RPO)	\$10,000 plus an additional \$10,000 per 4-hour period over the Max time allotted.
SLA-DR02	Recovery Time Objective (RTO)	\$10,000 plus an additional \$10,000 per 4-hour period over the Max time allotted.
SLA-DR03	Disaster Recovery Readiness	20.0%
SLA-DR04	After Action Reports	20.0%
SLA-DR05	Disaster Recovery Support	20.0%
SLA-DR06	Required periodical reporting	20.0%
SLA-DR07	CAP Failure	50.0%

#### E. Post-Award SLAs and KPIs

151. Post-Award KPI/SLA Overview - The Consortium States have identified specific post-award KPIs related to specific plans required as a part of the award of this RFP. The Vendor shall bear responsibility for the development of these plans. See Table 9 for the Post-Award SLAs/KPIs.

**Table 9 – Post-Award SLAs/KPIs**

Post-Award KPI Identifier	Post-Award KPI Name	Post-Award SLA Description
SLA-PA01	Sprint Velocity Establishment	The Vendor will establish a baseline sprint velocity within 180 days of the execution of the contract.
SLA-PA02	Staffing Capacity	The Vendor must illustrate how it will reach full capacity within ninety (90) days of the contract start date.
SLA-PA03	Baseline framework of plans	The Vendor will provide a baseline framework of the required plans (Enterprise Architecture Plan, Development and Quality Management Plan, Information Data Security Plan, Transition Plan, and Disaster Recovery Plan) within forty-five (45) days of the execution of the contract.
SLA-PA04	Expectation Document	The Vendor will provide an expectation document, outlining by section a proposed plan with detail for all major documents within forty-five (45) days of the execution of the contract.
SLA-PA05	Enterprise Architecture Plan	The Vendor will deliver an Enterprise Architecture Plan to the Consortium states within 180 days of the execution of the contract. The initial transition architecture “Technical Roadmap” must be included in the Enterprise Architecture Plan. The Vendor will work with each state’s business users to capture and document the high-level “Business Roadmap” as part of the Enterprise Architecture Plan. See

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

		SLA-012 for all future “Technical Roadmap” and “Business Roadmap” requirements.
<b>SLA-PA06</b>	Development and Quality Management Plan	The Vendor will deliver a development and quality management plan to the appropriate Consortium members within 180 days of the execution of the contract.  The Vendor will develop a Software Architecture plan that will align with the Enterprise Architecture Strategy to guide development efforts to evolve towards microservices and industry best practices with reference to those specific practices as part of the Development and Quality Management Plan.
<b>SLA-PA07</b>	Information and Data Security Plan	The Vendor will deliver a security plan to the appropriate Consortium members within 180 days of the execution of the contract. See SLA-012 for all future Information Data Security Plan requirements.
<b>SLA-PA08</b>	Transition Plan	The Vendor will deliver a transition plan at the schedule defined above.
<b>SLA-PA09</b>	Disaster Recovery Plan	The Vendor shall produce and deliver a baseline update form for ReEmployUSA Disaster Recovery Plan to the appropriate Consortium State within thirty (30) business days of the execution of the contract.
<b>SLA-PA10</b>	Code Quality Metrics	The Vendor will collaborate with each Consortium State on the acceptable metrics for code quality. These metrics must be established within ninety (90) days of the contract start date.
<b>SLA-PA11</b>	CAP Creation	The Vendor shall be required to prepare a CAP for any post Award SLA that exceeds the number of days for the requirements by more than sixty (60) days.
<b>SLA-PA12</b>	CAP Failure	The Vendor has shown an inability or failure to correct the CAP item from occurring. This is demonstrated by any SPA-PA’s being on a CAP for more than two (2) months.

#### **F. Post-Award KPI Failure and Maximum Penalties**

152. Post-Award KPI Failure - In the event specific Post-Award KPIs are not met, the applicable Consortium State, after documenting such failure, will follow the below guidelines. The percentages listed in Table 10 shall be applied for each 30 days that the Post-Award SLA/KPI exceeds the number of days for the requirements listed in each SLA-PA KPI. The Vendor shall be required to provide a CAP once the SLA-PA01 through SLA-PA10 exceeds sixty (60) days past the requirement.

- a. Right to Payment Reduction- If an individual state demonstrates a post-award KPI failure and elects to impose a penalty, as listed in Table 10, the penalty amount will be deducted from the next monthly Maintenance and Support invoice for that individual state.

SLA-PA01’s – SLA-PA12’s penalties may be assessed on a monthly basis up to the maximum penalty. See Table 10 for the Post-Award Maximum Penalties.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

- b. Maximum Payment Reduction Percentages - The maximum fees assessed must not exceed 100% of the applicable state’s monthly allocation of the annual UI Systems Maintenance and Support fees.
- c. In the event that the maximum payment reduction fees assessed equal or exceed 100% for any consecutive 2-month period, the Vendor may be deemed to be in breach of the Contract and may subject to Termination at the discretion of the individual Consortium States.

**Table 10 – Post-Award Maximum Penalties**

Post-Award KPI Identifier	Post-Award KPI Name	Maximum Payment Percentage Reduction
SLA-PA01	Sprint Velocity Establishment	20.0%
SLA-PA02	Staffing Capacity	20.0%
SLA-PA03	Baseline framework of Plans	20.0%
SLA-PA04	Expectation Document	20.0%
SLA-PA05	Enterprise Architecture Plan	20.0%
SLA-PA06	Development and Quality Management Plan	20.0%
SLA-PA07	Information Data Security Plan	20.0%
SLA-PA08	Transition Plan	20.0%
SLA-PA09	Disaster Recovery Plan	20.0%
SLA-PA10	Code Quality Metrics	20.0%
SLA-PA11	CAP Creation	20.0%
SLA-PA12	CAP Failure	50.0%

#### G. Audit and Compliance SLAs and KPIs

- 153. Audit and Compliance KPI/SLA Overview - In the event specific Audit and Compliance KPIs are not met, the applicable Consortium State, after documenting such failure, will follow the below guidelines.
- 154. Audit and Compliance KPIs/SLAs will be agreed upon by the Vendor and the Consortium. Additional KPIs/SLAs may be added by the Consortium. Table 11 provides the Audit and Compliance KPIs and SLA’s.

**Table 11 – Audit and Compliance SLAs/KPIs**

Audit and Compliance KPI Identifier	Audit and Compliance KPI Name	Audit and Compliance SLA Performance Standard
SLA-AC01	Annual SOCII Audit	<b>Performance Standard</b> The Vendor will undergo a yearly SOCII audit and ensure that the SOCII audit is completed by each state’s fiscal year end date.
SLA-AC02	Post-Award SOCII Audit	<b>Performance Standard</b> The Vendor will undergo a SOCII Audit within 90 days of the execution of the contract.
SLA-AC03	Vendor Participation in Audits	The Vendor must assist Consortium State(s) with federal and state audits, Vendor certifications, and other audits as the Consortium States deem necessary.

## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

		<p>The Vendor is required to comply with all audits as specified by Consortium States.</p> <p>The Vendor will provide full support of audits of the ReEmployUSA system along with any related systems, software, services, and tools.</p> <p><b>Performance Standard:</b> Actions or inactions of the Vendor that result in a delay, finding, or failure of any audit that is documented by the Consortium State(s) may result in a penalty as described above.</p>
<b>SLA-AC04</b>	CAP Failure	<p><b>Performance Standard:</b> The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 3 failures of the same SLA-DR within a 12-month period.</p>

#### H. Audit and Compliance KPI Failure and Maximum Penalties

155. In the event specific Audit and Compliance KPIs are not met, the applicable Consortium State, after documenting such failure, will follow the below guidelines. The percentages listed in Table 12 shall be applied for each 30 days that the Audit and Compliance SLA/KPI exceeds the number of days for the requirements listed in each SLA-AC KPI. The Vendor shall be required to provide a CAP once the SLA-AC01 or SLA-AC02 exceeds sixty (60) days past the requirement.
- a. Right to Payment Reduction- If an individual state demonstrates a post-award KPI failure and elects to impose a penalty, as listed in Table 12, the penalty amount will be deducted from the next monthly Maintenance and Support invoice for that individual state.
 

SLA-AC01's – SLA-AC04's penalties may be assessed on a monthly basis up to the maximum penalty. See Table 12 for the Audit and Compliance Maximum Penalties.
  - b. Maximum Payment Reduction Percentages - The maximum fees assessed must not exceed 100% of the applicable state's monthly allocation of the annual UI Systems Maintenance and Support fees.
156. In the event that the maximum payment reduction fees assessed equal or exceed 100% for any consecutive 2-month period, the Vendor may be deemed to be in breach of the Contract and may subject to Termination at the discretion of the individual Consortium States.

**Table 12 – Audit and Compliance Maximum Penalties**



## Attachment A

### RFP No. 4609 – ReEmployUSA Application Support, Corrective, Adaptive, Preventive, and Perfective Maintenance Services

Post-Award KPI Identifier	Post-Award KPI Name	Maximum Payment Percentage Reduction
SLA-AC01	Annual SOCII Audit	20.0%
SLA-AC02	Post-Award SOCII Audit	20.0%
SLA-AC03	Vendor Participation in Audits	20.0%
SLA-AC04	CAP Failure	50.0%

#### I. Corrective Action Plan

157. The Consortium States may request a Corrective Action Plan (CAP) when the Vendor fails to meet a required SLA. The Vendor shall provide the requesting Consortium State with a written CAP, submitted for approval by the appropriate Consortium State(s) no later than ten (10) business days from the date of the Consortium State's request for a CAP or other triggering event. Failure to provide a timely CAP upon request may result in a penalty assessment. See Tables 6, 8, 10, and 12 for Maximum Penalties, Disaster Recovery Maximum Penalties, Post-Award Maximum Penalties, and Audit and Compliance Maximum Penalties, SLA-017, SLA-DR07, SLA-PA12, and SPA-AC04.
158. CAP Failure - In the event of a CAP failure, the applicable Consortium State has the right to payment reduction based on predefined penalties.
- a. CAP Failure is defined as:
    - i. For KPI/SLAs: The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 3 failures of the same SLA within a 12-month period.
    - ii. For Disaster Recover KPI/SLAs: The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 3 failures of the same SLA-DR within a 12-month period.
    - iii. For Post-Award KPI/SLAs: The Vendor has shown an inability or failure to correct the CAP item from occurring. This is demonstrated by any SPA-PA's being on a CAP for more than two (2) months.
    - iv. For Audit and Compliance KPI/SLAs: The Vendor has shown an inability or failure to correct or prevent the CAP item from occurring. This is demonstrated by 2 failures of the same SLA-AC within a 12-month period.