REVISED ATTACHMENT I – KEY PERSONNEL REQUIREMENTS

List of Exhibits

Exhibit 1: CSC Project Director 3
Exhibit 2: CSC Manager 4
Exhibit 3: CSC Technical Lead 5
Exhibit 4: CSC Business Operations Lead 5
Exhibit 5: Security Officer 6
Exhibit 6: Privacy Officer 7
Exhibit 7: CSC Artificial Intelligence Lead 8

1 KEY PERSONNEL REQUIREMENTS

1.1 General

For the purpose of this Contract, the term “Key Personnel” refers to senior management and Contract personnel deemed by DHS to be essential to the satisfactory performance of this Contract. The Respondent shall provide candidate names for each Key Personnel Profile in their Response to the RFP. Sub-Contractor personnel may be identified as Key Personnel. All Key Personnel candidates shall meet the mandatory requirements for the proposed position as set forth in this document. DHS will not evaluate or score the recommended additions to the Key Personnel positions, but DHS must approve all candidates for recommended Key Personnel positions as if they were Key Personnel described in this Attachment.

Presence onsite in Little Rock, AR, may be required of Key Personnel at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/related activities.

The Respondent shall present a Key Personnel Profile Summary for each Key Personnel candidate. Key Personnel Summary Profiles shall be structured identically in format and layout for content.

1.1.1 Key Personnel Profile Summary Completion Information

The underlined texts serve as the Key Personnel Profile Summary completion guidelines.

1. *Education and Training*: Respondent shall list the relevant education and training of the proposed candidate and demonstrate, in detail, how a candidate’s education and training relates to their ability to perform the intended duties and obligations properly and successfully in this RFP.
2. *Required Experience and Qualifications*: The Respondent shall complete this section to show how the proposed candidate meets the experience requirements for the position.

   For each proposed candidate, the Respondent must provide the following profile information:
   - Full NAME of each previous project or engagement that shows how the candidate is qualified to perform the duties and obligations outlined in this RFP
   - Contact information for a reference from each project or engagement
   - Date(s) of experience with project or engagement
   - Description of duties on the project or engagement

1.1.2 Additional Completion Guidelines

1.1.2.1 Experience Dates

The Respondent shall provide the number of years of experience related to their assigned position for this project, including the beginning and end dates the candidate performed the job duties for each project or position. The details of their experience should include the position title or category of experience—technical, business or otherwise, as well as a detailed list of job duties. The date span must include both the beginning and end of the month and year. It is not sufficient to provide only the length of time the proposed candidate worked in the position or project.

DHS will not consider overlapping months of experience for a candidate as meeting or exceeding the Key Personnel Summary Profile "Mandatory Experience." It is acceptable to DHS that the Respondent's proposed candidates for this RFP collectively meet or exceed "Mandatory Experience" set forth. If the Respondent fails to submit a candidate as Key Personnel that can fulfill the mandatory experience, DHS may reject the Respondent's proposal as non-responsive.

1.1.2.2 Description of Duties

The Respondent shall customize the description of job duties for each listed project or position to clearly substantiate the proposed candidate's qualifications. Relevant experience should be clearly described and highlighted.

DHS will not assume that all skill set attributes or requirements descriptions provided relate identically to every technical skill set requirement. The candidate's work experience must be listed separately and completely each time it is referenced. Failure to provide this information or providing information that is inaccurate or out of date or client experience that is not applicable may result in DHS not including it in the evaluation process or rejecting the Respondent's proposal as non-responsive.

1.1.2.3 Resume

The Respondent must provide a Curriculum Vitae (CV) or resume for all individuals proposed as Key Personnel. The CV or resume must be no more than four (4) pages long, consistent in format, and in the same font size as that used for the body of the technical proposal. The resume must support the candidate's education, training, experience, and qualifications outlined in the Key Personnel Profile section above.

1.1.2.4 Exclusion of Sensitive Personal Information

It is the affirmative responsibility of the Respondent submitting a Proposal to remove all personal confidential information (such as home addresses and social security numbers) of Respondent staff and/or of any Sub-Contractor and Sub-Contractor's staff from resumes or any other part of the Proposal package.

Following submission to DHS, all Proposals submitted become part of the public record.

1.2 Non-Key Personnel

All personnel assigned by the Respondent to the performance of services under this RFP will be fully qualified to perform the duties required under the Contract. The Respondent must demonstrate its significant expertise in the remaining positions (non-Key Personnel) necessary to fulfill the requirements of this RFP.

2 KEY PERSONNEL POSITIONS

DHS identified a set of key personnel to be associated with this Contract. The positions described in this Section are required, based on the anticipated demands and the complexity of the solution. Positions denoted as key

personnel describe the role description rather than the specific title. The Contractor may rename roles, so long as all key personnel role requirements are fulfilled.

Due to the importance of these positions, DHS must approve in writing the assignment of a specific resource to these positions. The Respondent may not reassign or replace a named individual within Key Personnel without written approval of DHS.

The Respondent may recommend additional Key Personnel positions. In those cases, the Respondent must describe the general responsibilities associated with the position and the qualifications of the position based on best practice and current experience. Respondents may also nominate candidates for these positions. DHS will not evaluate or score the recommended additions to the Key Personnel positions, but DHS must approve all candidates for recommended Key Personnel positions as if they were Key Personnel described in this Attachment.

DHS identified the following key personnel positions for this Contract:

1. Customer Service Center (CSC) Project Director
2. CSC Manager
3. CSC Technical Lead
4. CSC Business Operations Lead
5. Security Officer
6. Privacy Officer
7. Artificial Intelligence Lead

2.1 CSC Project Director

The CSC Project Director is generally responsible for the following:

1. Overseeing the strategic direction and general management of the CSC responsibilities, including, but not limited to, management of the CSC Manager, CSC Technical Lead, Business Operations Lead, and support teams
2. Ensuring adherence to policies, procedures, and requirements, as outlined by the State, identifying business needs and maintaining updated business practices, in adherence with the requirements outlined in the Scope of Work
3. Acting as the principal interface for the CSC Vendor with the State
4. Allocating, scheduling and provisioning resources in accordance with the State and CSC needs
5. Presenting all formal CSC communication and correspondence to the State

The list above generalizes the responsibilities of the CSC Project Director and is not intended to be all inclusive. Exhibit 1 details the specific qualifications that are required of the individual assigned to the CSC Project Director position.

The CSC Vendor must designate in writing, and the State must pre-approve, an alternate for the CSC Project Director. Designation of an alternate is required before Project start-up. The alternate will serve as the Vendor's primary representative in the absence of the CSC Project Director and be expected to respond to the State, as necessary, when performing as the CSC Project Director.

Exhibit 1: CSC Project Director

CSC Project Director Qualifications
1. Possess a minimum of five (5) years of experience in managing or in a key management position for a large-scale customer service and/or CRM development project that encompasses the full system development life cycle from initiation through post-implementation. 2. Previous experience following a standard Project Management methodology and using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources. 3. Possess a current Project Management Professional (PMP) certification-. 4. Must have excellent communication skills, writing skills, small group facilitation skills, and formal presentation skills. 5. Previous Medicaid experience is required. 6. Previous CRM experience is required. 7. Possess a bachelor's degree in health care, business administration, information technology, or a related field; OR four (4) years of experience, in addition to the general requirement for five (5) years of experience, will be a suitable substitute for the bachelor's degree. 8. Presence onsite in Little Rock, AR, may be required at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/related activities.

2.2 CSC Manager

The list below generalizes the responsibilities of the CSC Manager and is not intended to be all-inclusive. The CSC Manager is generally responsible for the following:

1. Supervising and leading the daily operations of the CSC, including, but not limited to, overseeing quality assurance and quality improvement, managing, hiring and training the CSC workforce, and participating in testing and enhancement activities
2. Scheduling and provisioning resources to accomplish the CSC responsibilities
3. Identifying and mitigating project risks associated with software design, development, and implementation
4. Managing and reporting all service level agreements, performance standards and development status to the CSC Project Director
5. Monitoring and analyzing progress and performance of all projects, budgets, report delivery, and operations

Exhibit 2 identifies the specific qualifications required of the CSC Manager.

Exhibit 2: CSC Manager

CSC Manager Qualifications
1. Possess a minimum of five (5) years of experience in managing or in a key management position for a large-scale customer service and/or CRM project that encompasses the full system development life cycle from initiation through post-implementation. 2. Previous experience following a standard Project Management methodology and using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources. 3. Possess a current Project Management Professional (PMP) certification. 4. Must have excellent communication skills, writing skills, small group facilitation skills, and formal presentation skills. 5. Previous Medicaid experience is required.

CSC Manager Qualifications
6. Previous CRM experience is required. 7. Possess a bachelor's degree in health care, business administration, information technology, or a related field; OR four (4) years of experience, in addition to the general requirement for five (5) years of experience, will be a suitable substitute for the bachelor's degree. 8. Presence onsite in Little Rock, AR, may be required at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/related activities.

2.3 CSC Technical Lead

The list below generalizes the responsibilities of the CSC Technical Lead and is not intended to be all-inclusive. The CSC Technical Lead is generally responsible for the following:

1. Reviewing and assessing key project artifacts, including, but not limited to, design documents, test cases, project schedules against requirements and standards, and evaluating whether the State and Solution Vendor share a common understanding of the project scope, goals/outcomes/requirements, deliverables, and milestones
2. Performing testing assessments and validating test results
3. Identifying and mitigating technical project risks and implementing enhancements to the CSC
4. Making recommendations for the technical improvement of processes based on observations, industry standards, and best practices
5. Ensuring that all business and technical requirements are correctly incorporated into the Vendor's solution and monitoring progress toward certification/compliance

The CSC Technical Lead must be dedicated full-time to this project and cannot serve in any other position on this or any other contract or project. Specific requirements for the CSC Technical Lead are defined in Exhibit 3.

Exhibit 3: CSC Technical Lead

CSC Technical Lead Qualifications
1. Possess a minimum of five (5) years of experience in technical analyst and testing responsibilities on projects of similar scope. 2. Possess excellent communication skills, including writing skills. 3. Previous Medicaid experience is required. 4. Previous CRM experience is required. 5. Presence onsite in Little Rock, AR, may be required at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/project-related activities. 6. Possess a bachelor's degree or higher in a health care, business administration, or information technology related field; OR four (4) years of experience in similar industry, in addition to the general requirement for five (5) years of experience, will be a suitable substitute for the bachelor's degree.

2.4 CSC Business Operations Lead

The list below generalizes the responsibilities of the Business Operations Lead and is not intended to be all-inclusive. The Business Operations Lead is generally responsible for the following:

1. Ensuring that business rules and processes established by the Contractor are identified, documented and approved by DHS before and after system go-live
2. Overseeing CSC development and expansion activities, including, but not limited to, interviews with DHS divisions
3. Recommending improvements to business processes to ensure that the CSC enables cost savings and improved functionality to DHS through process improvement
4. Overseeing and consulting on change management practices with the Contractor and with DHS staff
5. Leading the development of the Interview Plan and Transfer of Operations Plan, as well as ongoing maintenance of stakeholder relationships to ensure the CSC expansion vision is executed

Specific requirements for the CSC Business Operations Lead are defined in Exhibit 4.

Exhibit 4: CSC Business Operations Lead

CSC Business Operations Lead
1. Possess a minimum of five (5) years of experience in management consulting and/or business analytics responsibilities on projects of similar scope. 2. Possess excellent communication skills, including writing skills. 3. Previous experience in change management is required. 4. Previous human services experience is required. 5. Must have knowledge of the Contractor's solution; having implemented and managed the solution in no less than one (1) environment at least as complex as the Contractor's solution. 6. Presence onsite in Little Rock, AR, may be required at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/project-related activities. 7. Possess a bachelor's degree or higher in a health care, business administration, or information technology related field; OR four (4) years of experience in similar industry, in addition to the general requirement for five (5) years of experience, will be a suitable substitute for the bachelor's degree.

2.5 Security Officer

The Security Officer shall provide advice on compliance matters, guiding management and staff in maintaining a compliant and secure operational environment. This position shall integrate compliance measures to ensure seamless adherence to security protocols. This position is responsible for assessing and enforcing all state and Federal mandated security policies.

The following list generalizes the responsibilities of the Security Officer and is not intended to be all inclusive:

1. Develop, maintain, document and report on the Contractor's security measures

2. Ensure the system complies with all current and future federal and state security regulations and standards
3. Conduct audits and implement safeguards to maintain data integrity and confidentiality
4. Lead initiatives to train Contractor and DHS employees, as requested, on compliance requirements and security best practices
5. Provides support for external security audits. The Security Officer position is not required to be onsite; however, DHS may require travel to the Contractor's primary facility for purpose of training, audits or compliance review.

Specific requirements for the Security Officer are defined in Exhibit 5.

Exhibit 5: Security Officer

Security Officer Qualifications
1. Possess a minimum of five (5) years of experience managing or in a key management position for a large-scale government human services project, including a minimum of three (3) years of experience as a Security officer. 2. Possess an expert knowledge of the Contractor's solution. 3. Must have excellent communication skills, writing skills, small group facilitation skills, and formal presentation skills. 4. Possess four (4) years of experience with MARS-E Security and compliance management, ARC-AMPE Security and Privacy Standards, NIST 800-53 controls, and/or CMS ARS. 5. Attend review meetings on-site as required by DHS. 6. Optional: Possess current ISACA Certified Information Security Manager (CISM), Certified in Cybersecurity (CC), OffSec Certified Professional (OSCP), OffSec Certified Professional Plus (OSCP+), Junior Penetration Tester (PT1), Practical SOC Analyst Associate (PSAA), Practical Web Pentest Associate (PWPA), Practical Web Pentest Professional (PWPP), Practical Junior Penetration Tester (PJPT), Practical Network Penetration Tester (PNPT), Certified Information Systems Security Professional (CISSP), and Certified Ethical Hacker (CEH).

2.6 Privacy Officer

The Privacy Officer shall provide advice on compliance matters, guiding management and staff in maintaining a compliant and confidential operational environment. This position shall integrate compliance measures to ensure seamless adherence to privacy protocols. This position is responsible for assessing and enforcing all state and Federal mandated Privacy policies.

The following list generalizes the responsibilities of the privacy Officer and is not intended to be all inclusive:

1. Develop, maintain, document and report on the Contractor's privacy measures
2. Ensure the system complies with all current and future federal and state privacy regulations and standards
3. Conduct audits and implement safeguards to maintain data integrity and confidentiality, specifically in regard to Protected Health Information (PHI) and Personally Identifiable Information (PII)
4. Lead initiatives to train Contractor and DHS employees, as requested, on compliance requirements and privacy best practices

5. Provides support for external privacy audits. The Privacy Officer position is not required to be onsite; however, DHS may require travel to the Contractor's primary facility for purpose of training, audits or compliance review.

Specific requirements for the Privacy Officer are defined in Exhibit 6.

Exhibit 6: Privacy Officer

Privacy Officer Qualifications
1. Possess a minimum of five (5) years of experience managing or in a key management position for a large-scale government human services project, including a minimum of three (3) years of experience as a Privacy Officer. 2. Possess an expert knowledge of the Contractor's solution. 3. Must have excellent communication skills, writing skills, small group facilitation skills, and formal presentation skills. 4. Attend review meetings on-site as required by DHS. 5. Optional: Possess current Certified Health Care Privacy and Security (CHPS) certification, Certified in Cybersecurity (CC), OffSec Certified Professional (OSCP), OffSec Certified Professional Plus (OSCP+), Junior Penetration Tester (PT1), Practical SOC Analyst Associate (PSAA), Practical Web Pentest Associate (PWPA), Practical Web Pentest Professional (PWPP), Practical Junior Penetration Tester (PJPT), Practical Network Penetration Tester (PNPT), Certified Information Privacy Professional (CIPP), and Certified Ethical Hacker (CEH).

2.7 CSC Artificial Intelligence Lead

The list below generalizes the responsibilities of the CSC Artificial Intelligence (AI) Lead and is not intended to be all-inclusive. The AI Lead is generally responsible for the following:

1. Developing the artificial intelligence implementation strategy, including but not limited to outlining roles and functionalities for AI within the CSC space, creating a road map for the implementation of AI tools, and identifying the State resources which could be the informational basis for the deployment of AI tools
2. Supervising the implementation of AI tools and AI-supported processes into the CSC space
3. Collaborating with the State to recommend opportunities to innovate the CSC through AI components
4. Overseeing the ongoing maintenance of live AI tools and processes, and ensuring that industry best practices are upheld
5. Establishing compliance protocols for AI use within the CSC space, including safeguarding data privacy and aligning with applicable laws and regulations

Specific requirements for the CSC AI Lead are defined in Exhibit 7.

Exhibit 7: CSC Artificial Intelligence Lead

CSC Artificial Intelligence Lead
1. Possess a minimum of five (5) years of experience leading artificial intelligence, data science, or machine learning projects of similar size. 2. Possess an expert knowledge of the Contractor's solution; having implemented and managed the solution in no less than one (1) environment at least as complex as the Contractor's solution.

3. Previous experience in technology adoption and business process transformation, with particular emphasis on incorporating artificial intelligence solutions into existing operational frameworks.

4. Possess excellent communication skills, including the ability to translate complex artificial intelligence concepts into clear, actionable information for stakeholders.

5. Presence onsite in Little Rock, AR, may be required at the discretion of the State. The percentage of time onsite will be determined depending on the nature of the project/project-related activities.

6. Possess a bachelor's degree or higher in computer science, data science, artificial intelligence, or a similar information technology related field.