



**STATE OF TENNESSEE  
CENTRAL PROCUREMENT OFFICE**

**REQUEST FOR QUALIFICATIONS  
FOR  
SYSTEMS INTEGRATION (SI) SERVICES  
RFQ # 32101-15557**

## TABLE OF CONTENTS

### SECTIONS:

1. Introduction
2. RFQ Schedule of Events
3. Response Requirements
4. General Information & Requirements
5. Procurement Process & Contract Award

### ATTACHMENTS:

- A. Technical Response & Evaluation Guide – Mandatory Requirement Items
- B. Technical Response & Evaluation Guide – General Qualifications & Experience Items
- C. Technical Response & Evaluation Guide – Technical Qualifications, Experience & Approach Items
- D. Cost Proposal & Evaluation Guide
  - D.1 Cost Proposal Workbook
- E. Statement of Certifications & Assurances
- F. Reference Questionnaire
- G. *pro forma* Contract
  - Attachment 1 – Attestation RE Personnel Used in Contract Performance
  - Attachment 2 – Liquidated Damages
  - Attachment 3 – List of Notices
  - Attachment 4 – Letter of Diversity Commitment
  - Attachment 5 – List of Interfaces
  - Attachment 6 – List of Reports
  - Attachment 7 – Definitions and Abbreviations
- H. Proposer’s Library
- I. Detailed Current State, Future State, and Roadmap Information
- J. Requirements Traceability Overview and Matrix
  - J.1 Functional Requirements
  - J.2 Non Functional Requirements
- K. Effort Workbook
- L. Optional DHS Expansion Phase
- M. HIPAA Business Associate Agreement
- N. Data Sources Information
- O. Additional SDLC and Operations and Maintenance Information

## 1 INTRODUCTION

The State of Tennessee, Central Procurement Office, hereinafter referred to as “the State,” has issued this Request for Qualifications (RFQ) to define mandatory goods or services requirements; solicit responses; detail response requirements; and, outline the State’s process for evaluating responses and selecting a Respondent for contract award to provide the needed goods or services.

Through this RFQ or any subsequent solicitation, the State seeks to buy the requested goods or services at the most favorable, competitive prices and to give ALL qualified businesses, including those that are owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises, the opportunity to do business with the state as contractors or subcontractors.

### 1.1 Statement of Procurement Purpose

- 1.1.1 The purpose of this RFQ is to solicit proposals for the design, development, testing, implementation, and for the operations and maintenance (O&M) of a new system to modernize and enhance eligibility determination, redetermination and eligibility appeals for the State of Tennessee’s Medicaid program (TennCare) and Children’s Health Insurance Program (CHIP, known as CoverKids in Tennessee).
- 1.1.2 The goal of the project is to modernize all aspects of Medicaid eligibility operations, enabling the State to administer all Medicaid eligibility determinations and related appeals functions. This modernization must improve processes currently undertaken, and also include taking over responsibility for eligibility determinations based on Modified Adjusted Gross Income (MAGI) that are currently performed by the Federally Facilitated Marketplace (FFM). Additionally, the project will leverage Service Oriented Architecture (SOA) principles to develop an extensible architecture that will comply with the Centers for Medicare and Medicaid Services’ (CMS) Medicaid Information Technology Architecture (MITA) 3.0, CMS’ Seven Conditions and Standards, and national standards for security, privacy, interoperability and information sharing.
- 1.1.3 The procurement and implementation of a single, streamlined eligibility determination system for Medicaid and CHIP, along with enhancements to the State’s eligibility determination and eligibility appeals processes, will enable the State to provide its residents with a seamless customer experience providing real-time or near real-time determination of eligibility for the majority of applicants. At the forefront of this effort is a “no wrong door” strategy that emphasizes efficiently capturing eligibility data electronically, regardless of how applicants choose to provide it, while promoting self-service and reducing transaction costs.
- 1.1.4 The Proposer will be required to sign the HIPAA Business Associate Agreement contained in RFQ Attachment M.

### 1.2 Pre-Response Conference

A Pre-Response Conference will be held at the time and date detailed in the RFQ Schedule of Events, RFQ § 2. Pre-Response Conference attendance is not mandatory, and potential Respondents may be limited to a maximum number of attendees depending upon overall attendance and space limitations. Please contact the Solicitation Coordinator to RSVP for the Pre-Response Conference. The Conference will be held at:

Bureau of TennCare  
 Division of Health Care Finance and Administration  
 310 Great Circle Road  
 Nashville, TN 37243

### 1.3 Notice of Intent to Respond

Before the Notice of Intent to Respond Deadline detailed in RFQ § 2, Schedule of Events, potential Respondents should submit to the Solicitation Coordinator, a Notice of Intent to Respond in the form of a simple e-mail or other written communication. Such notice should include the following information: the business or individual's name (as appropriate), a contact person's name and title, the contact person's mailing address, telephone number, facsimile number, and e-mail address. Filing a Notice of Intent to respond is not a prerequisite for submitting a response; however, it is necessary to ensure receipt of notices and communications relating to this RFQ.

### 1.4 Definitions and Abbreviations

Abbreviation	Definition
24/7/365	Available twenty-four (24) hours per day, seven (7) days per week, and three hundred sixty-five (365) days per year
ACCENT	Automated Client Certification and Eligibility Network for Tennessee
ACF	Administration for Children and Families
ACH	Automated Clearing House
AOA	Annual Operational Assessment
ATC	Authority to Connect
ATO	Authority to Operate
ATP	Account Transfer Process
BABOK	Business Analysis Body of Knowledge
BC/DR	Business Continuity and Disaster Recovery
BIA	Business Impact Analysis
BOM	Business Operating Model
BPM	Business Process Management
BRD	Business Requirements Document
BRE	Business Rules Engine
BRMS	Business Rules Management System
CAP	Corrective Action Plan
CD	Control Directive
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CI	Configuration Item
CIO	Chief Information Officer
CIP	Continuous Improvement Process
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CM	Control Memorandum
CMDB	Configuration Management Database
CMPPA	Computer Matching and Privacy Protection Act of 1988
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPO	Chief Privacy Officer
DAC	Disabled Adult Child
DB	Database
DBMS	Database Management System

<b>Abbreviation</b>	<b>Definition</b>
<b>DCS</b>	Department of Children's Services
<b>DDI</b>	Design, Development, and Implementation
<b>DED</b>	Deliverable Expectations Document
<b>DHS</b>	Department of Human Services (State of Tennessee)
<b>DIFSLA</b>	Disclosure of Information to Federal, State, and Local Agencies
<b>DNS</b>	Domain Name System
<b>DOH</b>	Department of Health
<b>DOJ</b>	Department of Justice
<b>DOLWD</b>	Department of Labor and Workforce Development
<b>DUNS</b>	Data Universal Numbering System
<b>EA</b>	Enterprise Architecture
<b>ECM</b>	Electronic Content Management
<b>ED</b>	Eligibility Determination
<b>ELC</b>	Enterprise Life Cycle
<b>EMP</b>	Eligibility Modernization Project
<b>EMPPA</b>	Eligibility Modernization Project Process Agreement
<b>EOG</b>	Eligibility Operations Group
<b>ERR</b>	Environment Readiness Review
<b>ESB</b>	Enterprise Service Bus
<b>ESM</b>	Enterprise System Modernization
<b>ETL</b>	Extract, Transform, and Load
<b>EVVE</b>	Electronic Verification of Vital Events
<b>FDSH</b>	Federal Data Services Hub
<b>FEIN</b>	Federal Employer Identification Number
<b>FFATA</b>	Federal Funding Accountability and Transparency Act
<b>FFM</b>	Federally Facilitated Marketplace
<b>FTE</b>	Full-time Equivalent
<b>FTI</b>	Federal Tax Information
<b>GIAC</b>	Global Information Assurance Certification
<b>GLBA</b>	Graham-Leach-Bliley Act of 1999
<b>Go-DBE</b>	Governor's Office of Diversity Business Enterprise
<b>GUI</b>	Graphical User Interface
<b>HCFA</b>	Division of Health Care Finance and Administration (State of Tennessee)
<b>HHS</b>	U.S. Department of Health and Human Services
<b>HIPAA</b>	Health Insurance Portability and Accountability Act of 1996
<b>HITECH</b>	Health Information Technology for Economic and Clinical Health Act
<b>ICD</b>	Interface Control Document
<b>IEA</b>	Information Exchange Agreement
<b>IMS</b>	Integrated Master Schedule
<b>IRC</b>	Internal Revenue Code
<b>IRR</b>	Implementation Readiness Review
<b>IRS</b>	Internal Revenue Service
<b>IS</b>	Information Systems
<b>ISA</b>	Interconnected Systems Agreement
<b>IT</b>	Information Technology
<b>ITIL</b>	Information Technology Infrastructure Library
<b>IV&amp;V</b>	Independent Verification and Validation

<b>Abbreviation</b>	<b>Definition</b>
<b>KPI</b>	Key Performance Indicator
<b>LAN</b>	Local Area Network
<b>LD</b>	Liquidated Damage
<b>LIS</b>	Low Income Subsidy
<b>LTSS</b>	Long Term Services and Supports
<b>O&amp;M</b>	Operations and Maintenance
<b>MAGI</b>	Modified Adjusted Gross Income
<b>MARS-E</b>	Minimum Acceptable Risk Standards for Exchanges
<b>MCO</b>	Managed Care Organization
<b>ME</b>	Medically Eligible
<b>MFA</b>	Multi-Factor Authentication
<b>MITA</b>	Medicaid Information Technology Architecture
<b>MMIS</b>	Medicaid Management Information System
<b>MMP</b>	Medicaid Modernization Program
<b>MOU</b>	Memorandum of Understanding
<b>MPI</b>	Master Person Index
<b>MSP</b>	Medicare Savings Program
<b>NAPHSIS</b>	National Association for Public Health Statistics and Information Services
<b>NCPD</b>	Notice of Calculation of Potential Damages
<b>NIAD</b>	Notice of Intent to Assess Damages
<b>NIST</b>	National Institute of Standards and Technology
<b>NOC</b>	Network Operations Center
<b>NPD</b>	Notice of Potential Damages
<b>NTP</b>	Network Time Protocol
<b>OASDI</b>	Old Age, Survivor, and Disability Insurance
<b>OCMT</b>	Organizational Change Management and Training
<b>OMB</b>	Office of Management and Budget
<b>OS</b>	Operating System
<b>OSSTMM</b>	Open Source Security Testing Methodology Manual
<b>PARIS</b>	Public Assistance Reporting Information System
<b>PHI</b>	Protected Health Information
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>PMI</b>	Project Management Institute
<b>PMLC</b>	Project Management Lifecycle
<b>PMO</b>	Project Management Office
<b>PMP</b>	Project Management Plan
<b>POA&amp;M</b>	Plan of Actions and Milestones
<b>PP</b>	Priority Population
<b>PPACA or ACA</b>	Patient Protection and Affordable Care Act, commonly referred to as Affordable Care Act
<b>QA</b>	Quality Assurance
<b>QI</b>	Qualified Individuals
<b>QM</b>	Quality Management
<b>RA</b>	Risk Assessment
<b>RFC</b>	Request for Change
<b>RFQ</b>	Request for Qualifications

<b>Abbreviation</b>	<b>Definition</b>
<b>RMF</b>	Risk Management Framework
<b>RPO</b>	Recovery Point Objective
<b>RTM</b>	Requirements Traceability Matrix
<b>RTO</b>	Recovery Time Objective
<b>SADD</b>	System Architecture Design Document
<b>SCA</b>	Security Control Assessment
<b>SDLC</b>	System Development Lifecycle
<b>SDX</b>	State Data Exchange
<b>SFTP</b>	Secure File Transfer Protocol
<b>SI</b>	System Integration
<b>SIT</b>	System Integration Testing
<b>SLA</b>	Service Level Agreement
<b>SLR</b>	Service Level Requirement
<b>SME</b>	Subject Matter Expert
<b>SMI</b>	Supplementary Medical Insurance
<b>SNAP</b>	Supplemental Nutrition Assistance Program
<b>SOA</b>	Service Oriented Architecture
<b>SOAP</b>	Simple Object Access Protocol
<b>SOP</b>	Standard Operating Procedure
<b>SP</b>	Special Publication
<b>SPMO</b>	Strategic Program Management Office
<b>SQL</b>	Structured Query Language
<b>SSA</b>	United States Social Security Administration
<b>SSI</b>	Supplemental Security Income
<b>SSN</b>	Social Security Number
<b>SSO</b>	Systems Security Officer
<b>SSP</b>	System Security Plan
<b>SSR</b>	Safeguard Security Report
<b>ST&amp;E</b>	Security Test and Evaluation
<b>STS</b>	Strategic Technology Solutions
<b>TANF</b>	Temporary Assistance for Needy Families
<b>TARB</b>	Technical Architecture Review Board
<b>TAS</b>	Technical Advisory Services
<b>TCA</b>	Tennessee Code Annotated
<b>TCCB</b>	Technical Change Control Board
<b>TCMIS</b>	TennCare Management Information System
<b>TCRS</b>	Tennessee Consolidated Retirement System
<b>TEAMS</b>	Tennessee Eligibility Appeals Management System
<b>TEDS</b>	Tennessee Eligibility Determination System, also known as Solution
<b>TMED</b>	Tennessee Medical Eligibility Determination System
<b>TNHC</b>	Tennessee Health Connection
<b>TOGAF</b>	The Open Group Architecture Forum
<b>TPL</b>	Third Party Liability
<b>UAT</b>	User Acceptance Testing
<b>USC</b>	United States Code
<b>USPS</b>	United States Postal Service
<b>VLP</b>	Verify Lawful Presence

Abbreviation	Definition
WAN	Wide Area Network
WBS	Work Breakdown Structure
WCAG	Web Content Accessibility Guidelines
WRS TN Tower	William R. Snodgrass Tennessee Tower
XML	Extensible Markup Language

Term	Definition
<b>Accessibility Testing</b>	Accessibility Testing is to ensure that the product is compliant with applicable Section 508 Accessibility and WCAG 2.0 AA Standards identified in the completed Section 508 Product Assessment. Software products (whether COTS, Government Off-the-Shelf, or custom-developed software applications) must adhere to Section 508 accessibility and other regulatory requirements governing the use of EIT in accordance with the CMS Policy for Section 508 Compliance. Accessibility Testing is required if the business application has a user interface or produces electronic output for direct access or use by federal employees or the public.
<b>Account transfers</b>	Automated process to receive applications originally entered through the Federally Facilitated Marketplace.
<b>Ad-hoc Testing</b>	Testing performed without planning and documentation where the tester tries to 'break' the system by randomly trying the system's functionality. Ad-hoc testing is typically informal and improvisational.
<b>Alert/monitoring Testing</b>	Alert/Monitoring Testing is the type of testing that is done where you purposely end test scenarios/cases in actions that would result in a system alert/message, ensuring that the correct actions are taken at that time. Alerts could be from a user perspective (telling the user that they provided the wrong SSN because it begins with 999), or on the system side (the system has received error code 01239, and the system appropriately handles that error code). Monitoring testing is that for known errors/messages, the system should be ready to monitor for those and intercept them and react to them appropriately.
<b>Beta Testing</b>	Beta testing of the Solution is run in a production environment and in parallel with the legacy production system. It allows a comparison of the results of processing between the legacy system and the new solution based on live data in the parallel production environments. It ensures that business sponsors are able to validate that the delivered solution in the target production environment supports all business requirements.
<b>Boundary Testing</b>	Boundary Testing consists of testing the extremes of the input domain, e.g., maximum, minimum, just inside/outside boundaries, typical values, and error values.
<b>Business Rules Management Tool</b>	Repository based on a defined strategy, allowing the defined rules to be managed in terms of versions and variants. The Businesses Rules Management tool shall be available to all relevant stakeholders to define and manage the business rules.
<b>Communication Management</b>	A component of the Project, Program, or Portfolio Management that describes how, when and by whom information about the project will be administered and disseminated.
<b>Compatibility Testing</b>	Compatibility Testing validates how well a software performs in a particular hardware/software/operating system/network environment. Backward Compatibility Testing tests the application or software in old or previous versions. Forward Compatibility Testing tests the application or software in new or upcoming versions.
<b>Component Integration Testing</b>	Component Integration Testing validates that all software components interact with one another correctly.
<b>Configuration Management</b>	Configuration Management includes the process of documenting formal procedures to apply technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a product, result, service, or component; control any changes to such characteristics; record and report each change and its implementation status; and support the audit of the products, results or components to verify conformance to requirements. It includes the documentation, tracking systems, and defined approvals necessary for authorizing and controlling changes.

<b>Term</b>	<b>Definition</b>
<b>Conversion Testing</b>	Conversion Testing is a testing process prescribed in the Data Conversion Plan that ensures testing is done in a manner reflective on how the system will be used in its "real" environment.
<b>Eligibility Modernization Project</b>	The Eligibility Modernization Project represent the State of Tennessee's highest priority in the Medicaid Modernization Program. The project's scope involves development and implementation of an eligibility determination system for TennCare and CHIP, which shall contain a rules-based decision engine, and that will be compliant with the Affordable Care Act, CMS requirements and all applicable State and Federal Regulations
<b>Eligibility Modernization Project Process Agreement</b>	The Eligibility Modernization Project Process Agreement (EMPPA) is used to authorize and document the justifications for using, not using, or combining specific Gate Reviews and the selection of specific deliverables applicable to the investment of Eligibility Modernization Project, including the expected level of detail to be provided. This document authorizes the project to proceed according to agreed upon scope, time, costs, and quality including any related exceptions as outlined within this document.
<b>Eligibility Modernization Project Steering Committee</b>	Members of the Eligibility Modernization Project Steering Committee shall be defined by the State.
<b>End-to-End Testing</b>	End-to-End Testing tests all of the business application's access or touch points, and data, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure business processes are successfully completed. Testing will be conducted on a complete, integrated set of business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly.
<b>Enterprise Testing</b>	Enterprise Testing tests all enterprise business applications that may have direct or indirect touch-points across multiple business applications and systems. Testing will be conducted on a complete, integrated set of enterprise business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly.
<b>Environment Readiness Review</b>	The Environment Readiness Review is a representation of the Validation Readiness Review, Implementation Readiness Review, and Production Readiness Review. These reviews are needed to enter the various CMS environments to test the solution and its contingency operations. Not all solutions will go through all environments. Specific requirements for running in each environment are provided by the environment's owner.
<b>Error Handling Testing</b>	Assesses the ability of the system to properly process erroneous transactions. The main objectives are to ensure that all reasonably anticipated error conditions are recognizable by the application system, accountability for processing errors has been assigned and that the procedures provide a high probability that the error will be properly corrected, and that reasonable control is maintained over errors during the correction process.
<b>Exploratory Testing</b>	Emphasizes the personal freedom and responsibility of the individual tester to continually optimize the quality of his/her work by treating test-related learning, test design, test execution, and test result interpretation as mutually supportive activities that run in parallel throughout the project.
<b>Failover Clustering</b>	Failover Clustering is a failsafe in which a two or more servers work together to ensure that if one (or more) fail, that another can seamlessly take over the workload without any downtime.
<b>Federal Facilitated Marketplace</b>	A CMS system providing consumer and small business access to a health insurance marketplace for states that have chosen not to build their own marketplace.
<b>Financial Management</b>	Financial Management is a process which brings together planning, budgeting, accounting, financial reporting, internal control, auditing, procurement, disbursement and the physical performance of the project with the aim of managing project resources properly and achieving the project's objectives. Like the concept of Project Management, it is a strategic competency for organizations and can make the difference between a successful project and audit reports.

<b>Term</b>	<b>Definition</b>
<b>Functional Requirement</b>	Functional requirements define the expected functionality of the product or Solution to be created.
<b>Functional Testing</b>	Assess the input/output functions of a business application against pre-defined functional and data requirements. Each and every functionality of the system is tested by providing appropriate input, verifying the output and comparing the actual results with the expected results. Types of functional testing include: Unit Testing, Smoke Testing, Sanity Testing, Integration Testing, White Box Testing, Black Box Testing, User Acceptance testing, Regression Testing
<b>Go-Live</b>	Successful implementation and deployment of all functionality aligned with a Release to the end-user population.
<b>Go/No-Go Decision</b>	Point at which a decision to continue or stop a course of action is made. If a decision is made to "go", this denotes that the solution conforms to the documented specifications.
<b>Human Resources Management</b>	A component of the Project Management Plan that describes how the roles and responsibilities, reporting relationships, and staff management will be addressed and structured.
<b>Implementation Readiness Review</b>	Gate Review to ensure the solution completed thorough Integration Testing and is ready for turnover to the formal, controlled test environment for Production Readiness.
<b>Interface Testing</b>	Interface Testing tests all of the business application's access or touch points, and data, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure business processes are successfully completed. Testing will be conducted on a complete, integrated set of business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly. This testing function is sometimes referred to as End-to-End Integration Testing.
<b>IV&amp;V Attestation</b>	IV&V Attestation is the process of establishing documented evidence that the solution does what it has been designed to do and will continue to operate correctly in the future. IV&V Attestation provides objective evidence that all software requirements have been implemented correctly and completely. This includes evidence that the solution produces the intended results and that all functionality is traceable to solution requirements.
<b>Gate Review</b>	<p>A Gate Review is a phase-driven go/no-go decision point where project activities are reviewed to assure that appropriate requirements are observed. A project cannot proceed without a Go decision by the appropriate senior management for a specific stage gate.</p> <p>Each Gate Review is an independent confirmation by the Gate Review Team (including relevant critical partners) to the IT Governance organization or delegated authority that all required project reviews have been successfully conducted. It checks that the TEDS Project Manager has satisfactorily produced all the required deliverables and met all exit criteria for a given SDLC phase to permit advancement to the next phase.</p> <p>The emphasis of the Gate Review is on:</p> <ol style="list-style-type: none"> <li>a) The successful accomplishment of SDLC phase objectives;</li> <li>b) The plans for the next life cycle phase; and</li> <li>c) The risks associated with moving into the next life cycle phase.</li> </ol> <p>The results of the Gate Review Team's assessment are provided with recommended action to the IT Governance organization or delegated authority for decision.</p>
<b>Go-Live</b>	Successful implementation and deployment of all functionality aligned with a Release to the end-user population.
<b>GUI Navigation Testing</b>	Validates the system logic behind when a user navigates from one screen to another. In a GUI system, at each time frame there is an active screen interacting with the user. The active screen, when triggered by specific event, will disappear or be deactivated and another one will be loaded in or activated. The two screens are logically connected by the event and such a scenario where the screen focus is shifted is called screen navigation.
<b>GUI Software Testing</b>	Testing through the use of a GUI, to ensure it meets agreed upon specifications as defined prior to software development. GUI testing evaluates design elements such as

<b>Term</b>	<b>Definition</b>
	layout, colors, fonts, font sizes, labels, text boxes, text formatting, captions, buttons, lists, icons, links, and content.
<b>MARS-E</b>	A document suite of guidance, requirements, and templates assembled by CMS. The document suite contains implementation standards for key security requirements contained in Department of Health and Human Services (HHS) ACA Regulations (45 CFR §§155.260 and 155.280) and other State and Federal regulations and policies. This is a harmonized set of guidelines inclusive of CMS and IRS requirements. Any reference to this package, even under CMS context references, should also infer compliance with current IRS Safeguards Program and IRS Pub 1075 where applicable by usage of data type and/or classification.
<b>Medicaid Modernization Program</b>	Medicaid Modernization Program is comprised of multiple sub-projects and is an initiative by the State of Tennessee to improve health care quality and access for members, achieve greater accountability for outcomes, create a more predictable and sustainable Medicaid budget, achieve more flexibility and scalability to meet the future needs of TennCare and CHIP program.
<b>Member Matching</b>	Determination if any given individual is a current Medicaid member (if they have a current Medicaid Plan)
<b>Member Portal</b>	The Member Portal shall provide Solution access to applicable insurance plan members or applicants.
<b>Negative Testing</b>	A Negative test will assess the response of the system outside of normal parameters and is designed to assess the system's ability to successfully perform error handling with the unexpected input. The tester uses invalid inputs or imitates unexpected user behavior to expose potential errors and system risk.
<b>Non-Functional Requirement</b>	Non-functional Requirements define the specific technical functionality that must exist in the Solution to deliver the business functionality, the operational objectives of the Solution, and the methodology and processes to manage the Solution delivery.
<b>Operational Readiness Testing</b>	Ensure that the operational readiness is appropriately comprehensive and inclusive of all elements of the State enterprise impacted by the TEDS deployment. Operational readiness may include checking the backup/restore facilities, IT disaster recovery procedures, maintenance tasks, and periodic check of security vulnerabilities.
<b>Partner Portal</b>	The Partner Portal shall provide Solution access to current TennCare Pre-Admission Evaluation System users, nursing homes, and hospitals. The Partner Portal shall be accessible both within the State of Tennessee network, and outside of the State of Tennessee network.
<b>Performance Management</b>	Performance Management is the use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform resources to either confirm or change current policy or program directions to meet those goals, and report on the success in meeting those goals.
<b>Performance Testing</b>	Assesses the capacity and throughput of a business application and/or infrastructure in processing time, CPU utilization, network utilization, and memory and storage capacities relative to expected normal (average and peak) user and processing load as defined in the system's requirements document and/or Operation Manual document.
<b>Production Instance</b>	Denotes the version of the code that is in operation.
<b>Quality Control Testing</b>	Testing that determines if the solution is performing and adheres to the predetermined requirements and expectations. The testing will verify the solution was developed as outlined in the documented requirements.
<b>Quality Management</b>	Quality Management includes the process and activities of performing organization that determine quality policies, objectives, and responsibilities so that the project will satisfy the needs for which it was undertaken. Quality Management uses policies and procedures to implement, within the project's context, the organization's quality management system and, as appropriate, it supports continuous process improvement activities as undertaken on behalf of the performing organization.
<b>Release</b>	A Release is the distribution of the updated version of the solution. Release can be a stage in development of a solution or maturity for a piece of software: ranging from its initial development to its eventual release, and including updated versions of the released version to help improve software or fix bugs still present in the solution.
<b>Recovery Testing</b>	Validates how well an application is able to recover from crashes, hardware failures,

Term	Definition
	and other similar problems. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
<b>Regression Testing</b>	Selective re-testing to validate that modifications have not caused unintended functional or data results and that the application still complies with its specific requirements.
<b>Reliability Testing</b>	Monitor the operational availability of business applications and/or infrastructure, problems/incidents, performance/service level, and capacity utilization of production systems, and will validate the gathered data against expected results (documented in the system's requirement document and/or Operation Manual document) to ensure that the implemented application or infrastructure performs as expected in production. This testing function is sometimes referred to as Reliability Validation, Burn in Period, Reliability Test, or Extended Reliability Test.
<b>Requirements Management Tool</b>	Repository based on a defined strategy, identifying the relationship, interface, or dependency on data in other tools. A Requirements Management tool will describe how the traceability strategy and how the requirements will be structured.
<b>Requirements Traceability Matrix</b>	A grid that links product requirements from their origin to the deliverables that satisfy them. The implementation of Requirements Traceability Matrix helps ensure that each requirement adds business value by linking it to the business and project objectives. It provides a means to track requirements throughout the project lifecycle, helping to ensure that requirements approved in the requirements documentation are delivered at the end of the project. Finally, it provides a structure for managing changes to the scope.
<b>Risk and Issue Escalation</b>	Process of identifying time frames and the management chains (names) for escalation of issues and risks that cannot be resolved at a lower staff level.
<b>Risk Management Framework (RMF)</b>	Framework required by the State of Tennessee to inform, advise, and manage the activities of security categorization (as defined in the federal publication FIPS 199), security control selection and implementation, security control assessment, information system authorization (ATO and ATC), and security control monitoring. The State must approve the RMF and it must meet standard practices associated with effective implementation, management, and maintenance of the NIST RMF.
<b>Scalability</b>	Identify major workloads and mitigate bottlenecks that can impede the scalability of the application. Scalability testing is a subset of performance testing. Performance testing can be used to establish a baseline against which future performance tests can be compared against.
<b>Schedule Management</b>	Schedule Management is a subsidiary of, and integrated with, the Project Management Plan. Schedule Management identifies a scheduling method and scheduling tool and sets the format and establishes criteria for developing and controlling the project schedule. The selected scheduling method defines the framework and algorithms used in the scheduling tool to create the schedule model.
<b>Scope Management</b>	Scope Management is a discipline of Project Management that defines how the project scope will be defined, validated and controlled. The key benefit of the process is that it provides guidance on how scope will be managed throughout the project.
<b>Security and Privacy Controls</b>	<p>The security and privacy controls that apply to information assets, in principal, are commensurate with the potential impact on information assets, organizational operations, or individuals, should there be a compromise of confidentiality, integrity, or availability of the information. Federal and State regulations and policies define specific classifications of data that require specific levels of control. In some instances, such as FTI, the source of the data is a factor in determining the security and privacy controls that apply to data elements. Security and privacy controls shall include, at a minimum:</p> <ol style="list-style-type: none"> <li>a) Role based access</li> <li>b) Data ownership/authorization rights</li> <li>c) MFA – when a third party accesses sensitive information about another person</li> <li>d) Encryption of information in transit</li> <li>e) Encryption of information at rest</li> <li>f) Data masking/synthetic data requirements</li> <li>g) Secure file transfers</li> </ol>

Term	Definition
	<ul style="list-style-type: none"> <li>h) Masking of data elements on displays or reports (for example, replacing all but the last four digits of a key person identifier such as an SSN)</li> <li>i) Recording an audit trail of who accesses what specific sensitive data and when</li> <li>j) Training</li> <li>k) Classification of the data, with respect to sensitivity of content and source governance, drives the security and privacy controls for the data. This is a key activity that shall be completed to the approval of the State Chief Security Officer, Chief Privacy Officer (CPO), and other stakeholders at project initiation. This classification serves as the foundation for security activities throughout the SDLC.</li> </ul>
<b>Security and Privacy Management Tools</b>	<p>The State requires management of security and privacy in compliance with Federal and State regulations and policies. The Contractor shall provide the expertise to utilize these tools throughout the SDLC for the project, including, at a minimum:</p> <ul style="list-style-type: none"> <li>l) Database Security Monitoring and Compliance Reporting (Oracle Audit Vault or functional equivalent)</li> <li>m) Vulnerability Scan (Nessus or functional equivalent)</li> <li>n) Security Information and Event Management (Qradar or functional equivalent)</li> <li>o) Static Code Checking (Fortify or functional equivalent)</li> <li>p) Log Server (SysLog Server or functional equivalent)</li> <li>q) File Integrity Checker (Advanced Intrusion Detection Environment or functional equivalent)</li> <li>r) Virus Scan (Symantec Endpoint Protection (Windows), Clam Antivirus (Linux), or functional equivalent)</li> <li>s) Compliance and Information Security Program Management (Lockpath Keylight or functional equivalent)</li> <li>t) Identity and Access Management (Oracle Identity and Access Management or functional equivalent)</li> <li>u) System Monitoring (Sitescope or functional equivalent)</li> <li>v) Application Scanning (NetSparker Server or functional equivalent)</li> </ul>
<b>Security Compliance Testing</b>	<p>A Security Test &amp; Evaluation (ST&amp;E) will validate all applicable security controls defined in the CMS Policy for the Information Security Program. ST&amp;E validates that business application or infrastructure are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the application or infrastructure. ST&amp;E may include vulnerability scanning, penetration testing, and/or testing security standards and policy.</p>
<b>Security Control Assessment</b>	<p>Addresses how the evaluator shall perform active security testing of the information system to assess the implemented security controls and to identify gaps between the implemented controls and the documented controls. The evaluator shall capture, document and retain information sufficient to prove the existence or non-existence of vulnerabilities discovered through the assessment process. Any gaps identified during the documentation review, interviews or security control assessments will be reported in the findings report based on the CMS Reporting Procedure for Information Security Assessments.</p>
<b>Smoke/Sanity Testing</b>	<p>Smoke Tests are shallow and wide, testing all areas of the application without getting deep in focus. Sanity tests are narrow and deep regression tests, testing one or a few areas of functionality. These tests are used to determine if an environment or Release is stable enough to begin a testing cycle.</p>
<b>Solution or System</b>	<p>Solution (or System) describes features, functions, and characteristics of the product, system, service, or result that will meet the business and stakeholder requirements.</p>
<b>Stakeholder Management Process</b>	<p>The Stakeholder Management Process is used to identify the project's key stakeholders and their roles and responsibilities within the project, provide an analysis of their interests in and attitude towards the effort, and manage stakeholder participation to secure positive support for the project. The Stakeholder Management process capability identifies the impacted groups or individuals and their needed level of commitment and establishes detailed engagement plans for impacted stakeholders</p>

Term	Definition
	to ensure project success.
<b>Successful Release</b>	All designed capabilities are operational according to specification and the State accepts the Go-Live deliverable
<b>Technical Sandbox</b>	The Technical Sandbox is an isolated and restricted computer environment where developers conduct testing on untested and untrusted codes. A restricted environment is created to ensure stability and security
<b>Test Management Tool</b>	Repository for all test documents, cases, results, statues, and how testing was done. The testing repository will include all automated and manual activities.
<b>Time-travel</b>	Ability to future-date or back-date operating system date in order to assist in testing of functionality related to time-driven events.
<b>Unit Testing</b>	Unit Testing is performed by the system developer/maintainer subsequent to or in parallel with application development to assess and correct the functionality and data of a business application's individual code modules.
<b>Usability Testing</b>	Testing technique typically performed by end users to verify the appropriate level of ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component.
<b>User Acceptance Testing</b>	Assess and accept the overall functionality and interoperability of a business application's Solution in an operational mode. UAT allows end users to use the Solution in a manner that most resembles actual production use. Testing is performed against the Business Product/Code based on the user's requirements, and may include Training Artifacts and User Manual. UAT may also assess the user's experience with the application to determine if users are able to accomplish their tasks and goals satisfactorily and efficiently to help identify potential problems and possible improvements (i.e., usability testing). Success in UAT will result in a sign-off by the business owner, validating that the business application meets documented requirements.
<b>Worker Portal</b>	The Worker Portal shall provide Solution access to member services workers, appeals unit workers, service center staff (TNHC intake, including intake for CHIP & the Redetermination Vendor), State office users outside of member services, including internal audit, policy, fiscal, and help desk, Department of Children's Services (Foster Care), and other Department of Health (DOH) application intake. The Worker Portal shall be accessible both within the State of Tennessee network, and outside of the State of Tennessee network.

## 2 RFQ SCHEDULE OF EVENTS

### 2.1 RFQ Schedule

The following schedule represents the State's best estimates for this RFQ; however, the State reserves the right, at its sole discretion, to adjust the schedule at any time, or cancel and reissue a similar solicitation. Nothing in this RFQ is intended by the State to create any property rights or expectations of a property right in any Respondent.

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFQ Issued		04/01/2016
2.	Disability Accommodation Request Deadline		04/06/2016
3.	Pre-Response Conference	2:00 p.m.	04/08/2016
4.	Notice of Intent to Respond Deadline		04/11/2016
5.	Written "Questions & Comments" Deadline	12:00 p.m.	04/15/2016
6.	State response to written "Questions & Comments"		04/29/2016
7.	RFQ Technical Proposal Deadline	11:00 a.m.	05/27/2016
8.	State Schedules Respondent Oral Presentations (ONLY Respondents who pass Mandatory Requirements)		06/06/2016
9.	Respondent Oral Presentation	8:00 a.m. – 4:30 p.m. Central Standard Time	06/27/2016 – 06/30/2016
10.	Open Cost Proposals		07/05/2016
11.	RFQ Cost Negotiations		July 7 – July 11, 2016
12.	State Evaluation Notice Released	2:00 p.m.	07/15/2016
13.	Solicitation Files Opened for Public Inspection		07/18/2016
14.	Respondent Contract Signature Deadline		08/04/2016
15.	Contract Start Date		09/01/2016

### 3 RESPONSE REQUIREMENTS

#### 3.1 Response Contents: A response to this RFQ should address the following:

- 3.1.1 **Mandatory Requirements:** This section details the mandatory technical, functional, and experience requirements that must be demonstrated in the response to this RFQ in order to be passed on to Stage II of the Technical Response evaluation. A Respondent must duplicate and use RFQ Attachment A as a guide to organize responses for the Mandatory Requirements of the RFQ response. The Respondent should reference the page location of the information within the response in the indicated column of the table. This section is included in the State's evaluation as to whether or not a Respondent meets mandatory qualifications. (Stage I)
- 3.1.2 **General Qualifications & Experience:** This section is included in the State's evaluation of Stage II of the Technical Response Evaluation and details general information and qualifications that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment B as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.
- 3.1.3 **Technical Qualifications, Experience & Approach:** This section is also included in the State's evaluation of Stage II of the Technical Response Evaluation and details technical qualifications, experience, and approach items that must be demonstrated in the response to this RFQ. A Respondent must duplicate and use RFQ Attachment C as a guide to organize responses for this portion of the RFQ response. The Respondent should reference the page location in the information within the response in the indicated column of the table.
- 3.1.4 **Cost Proposal**
- 3.1.4.1 The Cost Proposal must be submitted with the Technical Proposal and must be recorded on an exact duplicate of RFQ Attachment D and D.1, Cost Proposal & Evaluation Guide and Cost Proposal Excel Spreadsheet. Any response that does not follow the instructions included in RFQ Attachment D and D.1 may be deemed nonresponsive.
- 3.1.4.2 A Respondent must only record the proposed cost exactly as required by the RFQ Attachment D and D.1, Cost Proposal & Evaluation Guide and Cost Proposal Excel Spreadsheet, and must NOT record any other rates, amounts, or information.
- 3.1.4.3 The proposed cost shall incorporate ALL costs for services under the contract for the total contract period.
- 3.1.4.4 A Respondent must sign and date the Cost Proposal.
- 3.1.4.5 A Respondent must submit the Cost Proposal to the State in a sealed package separate from the Technical Response.

#### 3.2 Response Delivery Location

A Respondent must ensure that the State receives a Response to this RFQ no later than the Response Deadline time and dates detailed in the RFQ § 2, Schedule of Events. All responses must be delivered to:

Nicholas Edwards – Sourcing Analyst

Department of General Services

312 Rosa L. Parks Ave., WRS TN Tower, 3<sup>rd</sup> Floor

Nashville, TN 37243

Telephone: 615-741-1075

Email: [nicholas.edwards@tn.gov](mailto:nicholas.edwards@tn.gov)

### 3.3 Response Format

3.3.1 A Respondent must ensure that the original response meets all form and content requirements detailed within this RFQ.

3.3.2 A Respondent must submit original response documents and copies as specified below.

#### 3.3.2.1 Technical Response

One (1) original Technical Response paper document clearly labeled:

**“RFQ #32101-15557 TECHNICAL RESPONSE ORIGINAL”**

and five (5) copies of the Technical Response each in the form of one (1) digital document in Adobe Portable Document Format properly recorded on its own otherwise blank, standard CD-R recordable disc, or USB flash drive labeled:

**“RFQ #32101-15557 TECHNICAL RESPONSE COPY”**

The digital copies should not include copies of sealed customer references or cost information in the general and technical evaluation stage. However, any other discrepancy between the paper response document and digital copies may result in the State rejecting the response as nonresponsive.

#### 3.3.2.2 Cost Proposal

One (1) original Cost Proposal paper document labeled:

**“RFQ #32101-15557 COST PROPOSAL ORIGINAL”**

and one (1) copy in the form of a digital document in “XLS” format properly recorded on a separate, blank, standard CD-R recordable disc, or USB flash-drive labeled:

**“RFQ #32101-15557 COST PROPOSAL COPY”**

In the event of a discrepancy between the original Cost Proposal document and the digital copy, the original, signed document will take precedence.

### 3.4 Response Prohibitions: A response to this RFQ shall not:

3.4.1 Restrict the rights of the State or otherwise qualify the response to this RFQ;

3.4.2 Include, for consideration in this procurement process or subsequent contract negotiations, incorrect information that the Respondent knew or should have known was materially incorrect;

3.4.3 Include more than one response, per Respondent, to this RFQ;

3.4.4 Include any information concerning costs (in specific dollars or numbers) associated with the Technical Response;

- 3.4.5 Include the respondent's own contract terms and conditions (unless specifically requested by the RFQ); or
- 3.4.6 Include the respondent as a prime contractor while also permitting one or more other respondents to offer the respondent as a subcontractor in their own responses.

### **3.5 Response Errors & Revisions**

A Respondent is responsible for any and all errors or omissions in its response to this RFQ. A Respondent will not be allowed to alter or revise its response after the Response Deadline time and dates as detailed in RFQ § 2, Schedule of Events, unless such is formally requested in writing by the State (e.g., through a request for clarification, etc.).

### **3.6 Response Withdrawal**

A Respondent may withdraw a response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events, by submitting a written signed request by an authorized representative of the Respondent. After withdrawing a response, a Respondent may submit another Response at any time before the Response Deadline time and date as detailed in RFQ § 2, Schedule of Events.

### **3.7 Response Preparation Costs**

The State will not pay any costs associated with the preparation, submittal, or presentation of any response. Each Respondent is solely responsible for the costs it incurs in responding to this RFQ.

## 4 GENERAL INFORMATION & REQUIREMENTS

### 4.1 Communications

- 4.1.1 Respondents shall reference RFQ #32101-15557 in all communications relating to this solicitation, and direct any such communications to the following person designated as the Solicitation Coordinator:

Nicholas Edwards – Sourcing Analyst  
 Department of General Services  
 312 Rosa L. Parks Ave., WRS TN Tower, 3<sup>rd</sup> Floor  
 Nashville, TN 37243  
 Telephone: 615-741-1075  
 Email: [nicholas.edwards@tn.gov](mailto:nicholas.edwards@tn.gov)

The State will convey all official responses and communications related to this RFQ to the potential respondents from whom the State has received a Notice of Intent to Respond (refer to RFQ Section 1.3).

- 4.1.2 Potential respondents with a handicap or disability may receive accommodation relating to the communication of this RFQ and participating in the RFQ process. Potential respondents may contact the RFQ Coordinator to request such reasonable accommodation no later than the Disability Accommodation Request Deadline detailed in RFQ § 2.0, Schedule of Events.

- 4.1.3 **Unauthorized contact about this RFQ with other employees or officials of the State of Tennessee may result in disqualification from contract award consideration.**

- 4.1.4 Notwithstanding the foregoing, potential Respondents may also contact the following as appropriate:

- 4.1.4.1 Staff of the Governor's Office of Diversity Business Enterprise may be contacted for assistance with respect to available minority-owned, woman-owned, Tennessee service-disabled veteran-owned, and small business enterprises as well as general public information relating to this request; or

- 4.1.4.2 The following individual designated by the State to coordinate compliance with the nondiscrimination requirements of the State of Tennessee, Title VI of the Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, and associated federal regulations:

Talley A. Olson  
 Director, Office of Civil Rights Compliance  
 Division of Health Care Finance and Administration  
 310 Great Circle Road, 4 West  
 Nashville, TN 37243  
 Phone: 615- 507-6841  
 Email: [Talley.A.Olson@tn.gov](mailto:Talley.A.Olson@tn.gov)  
 Fax 615- 532-7322

## 4.2 Nondiscrimination

No person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of a contract pursuant to this solicitation or in the employment practices of the Vendor on the grounds of handicap or disability, age, race, color, religion (subject to Tennessee Code Annotated, Sections 4-21-401 and 405), sex, national origin, or any other classification protected by federal, Tennessee state constitutional, or statutory law. The Vendor pursuant to this solicitation shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

## 4.3 Conflict of Interest

4.3.1 The State may not consider a proposal from an individual who is, or within the past six (6) months has been, a State employee. For these purposes:

4.3.1.1 An individual shall be deemed a State employee until such time as all compensation for salary, termination pay, and annual leave has been paid;

4.3.1.2 A contract with or a proposal from a company, corporation, or any other contracting entity in which a controlling interest is held by any State employee shall be considered to be a contract with or proposal from the employee; and

4.3.1.3 A contract with or a proposal from a company, corporation, or any other contracting entity that employs an individual who is, or within the past six months has been, a State employee shall not be considered a contract with or a proposal from the employee and shall not constitute a prohibited conflict of interest.

4.3.2 This RFQ is also subject to *Tennessee Code Annotated*, Section 12-4-101.

## 4.4 Respondent Required Review & Waiver of Objections

4.4.1 Each potential respondent must carefully review this RFQ, including but not limited to, attachments, the RFQ Attachment G, pro forma Contract, and any amendments for questions, comments, defects, objections, or any other matter requiring clarification or correction (collectively called "questions and comments").

4.4.2 Any potential respondent having questions and comments concerning this RFQ must provide such in writing to the State no later than the written "Questions & Comments Deadline" detailed in RFQ § 2.0, Schedule of Events.

4.4.3 Protests based on any objection shall be considered waived and invalid if the objection has not been brought to the attention of the State, in writing, by the written "Questions & Comments Deadline."

## 4.5 Disclosure of Response Contents

4.5.1 All materials submitted to the State in response to this solicitation become property of the State of Tennessee. Selection for award does not affect this right. By submitting a response, a Respondent acknowledges and accepts that the full contents and associated documents submitted in response to this request will become open to public inspection. Refer to RFQ § 2.0, Schedule of Events.

4.5.2 The RFQ responses will be available for public inspection only after the completion of evaluation of the RFQ or any resulting solicitation which this RFQ becomes a part of, whichever is later.

#### **4.6 Notice of Professional Licensure, Insurance, and Department of Revenue Registration Requirements**

- 4.6.1 All persons, agencies, firms or other entities that provide legal or financial opinions, which a Respondent provides for consideration and evaluation by the State as part of a response to this RFQ, shall be properly licensed to render such opinions.
- 4.6.2 Before the Contract resulting from this RFQ is signed, the apparent successful Respondent (and Respondent employees and subcontractors, as applicable) must hold all necessary, appropriate business and professional licenses to provide service as required. The State may require any Respondent to submit evidence of proper licensure.
- 4.6.3 Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must provide a valid, Certificate of Insurance indicating current insurance coverage meeting minimum requirements as may be specified by the RFQ.
- 4.6.4 Before the Contract resulting from this RFQ is signed, the apparent successful Respondent must be registered with the Department of Revenue for the collection of Tennessee sales and use tax. The State shall not approve a contract unless the Respondent provides proof of such registration. The foregoing is a mandatory requirement of an award of a contract pursuant to this solicitation.

#### **4.7 RFQ Amendments & Cancellation**

- 4.7.1 The State reserves the right to amend this RFQ at any time, provided that it is amended in writing. However, prior to any such amendment, the State will consider whether it would negatively impact the ability of potential respondents to meet the deadlines and revise the RFQ Schedule of Events if deemed appropriate. If a RFQ amendment is issued, the State will convey it to potential respondents who submitted a Notice of Intent to Respond (refer to RFQ §1.3) A respondent must respond, as required, to the final RFQ (including its attachments) as may be amended.
- 4.7.2 The State reserves the right, at its sole discretion, to cancel or to cancel and reissue this RFQ in accordance with applicable laws and regulations.

#### **4.8 State Right of Rejection**

- 4.8.1 Subject to applicable laws and regulations, the State reserves the right to reject, at its sole discretion, any and all proposals.
- 4.8.2 The State may deem as nonresponsive and reject any proposal that does not comply with all terms, conditions, and performance requirements of this RFQ. Notwithstanding the foregoing, the State reserves the right to seek clarifications or to waive, at its sole discretion, a response's minor variances from full compliance with this RFQ. If the State waives variances in a response, such waiver shall not modify the RFQ requirements or excuse the Respondent from full compliance with such, and the State may hold any resulting vendor to strict compliance with this RFQ.

- 4.8.3 The State will review the response evaluation record and any other available information pertinent to whether or not each respondent is responsive and responsible. If the evaluation team identifies any respondent that appears not to meet the responsive and responsible thresholds such that the team would not recommend the respondent for potential contract award, this determination will be fully documented for the record. ("Responsive" is defined as submitting a response that conforms in all material respects to the RFQ. "Responsible" is defined as having the capacity in all respects to perform fully the contract requirements, and the integrity and reliability which will assure good faith performance.)

#### **4.9 Assignment & Subcontracting**

- 4.9.1 The vendor may not subcontract, transfer, or assign any portion of the Contract awarded as a result of this RFQ without prior written approval of the State. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment.
- 4.9.2 If a Respondent intends to use subcontractors, the response to this RFQ must specifically identify the scope and portions of the work each subcontractor will perform (refer to RFQ Attachment B, Item 14).
- 4.9.3 Subcontractors identified within a response to this RFQ will be deemed as approved by the State unless the State expressly disapproves one or more of the proposed subcontractors prior to signing the Contract. The State reserves the right to revoke approval for subcontractors approved under this section.
- 4.9.4 The Contractor resulting from this RFQ may only substitute another subcontractor for a proposed subcontractor at the discretion of the State and with the State's prior, written approval given after review of the Contractor's proposed subcontract.
- 4.9.5 Notwithstanding any State approval relating to subcontracts, the Contractor resulting from this RFQ will be the prime contractor and will be responsible for all work under the Contract.

#### **4.10 Next Ranked Respondent**

The State reserves the right to initiate negotiations with the next ranked respondent should the State cease doing business with any respondent selected via this RFQ process.

## 5 PROCUREMENT PROCESS AND CONTRACT AWARD

- 5.1 The complete vendor selection will be a two-part process: (1) Qualification of Technical Responses; and (2) Evaluation of Cost Proposals. Any contract award is subject to successful contract negotiation.
- 5.2 Qualification of Technical Responses: Technical Responses will be short-listed for further evaluation, analysis or negotiation if they are apparently responsive, responsible, and within the competitive range. A Technical Response will be deemed within the competitive range based on the following criterion:
- 5.2.1 The State seeks a vendor who can meet its need for a modernized eligibility system. All vendors must demonstrate sufficient competency in all components of the technical evaluation criteria. Vendors who do not meet the minimum sufficiency for the technical evaluation response section will be eliminated from consideration. Although price is an important consideration for the State, the State will not consider vendors whose responses do not demonstrate sufficient capabilities in all key areas within this proposal. In order for a vendor to demonstrate sufficient capabilities in all key areas of this proposal, the vendor must receive a minimum of 70% (630 total points) of the total combined points for the combined Technical Sections stated in RFQ Section 5.5. Proposals with Combined Scores of less than 630 points will not qualify for further consideration. In the event that no offer proceeds to the cost evaluation stage, the State reserves the right to lower the sufficiency threshold. Any change to the sufficiency threshold will be applied consistently to all respondents.
- 5.2.2 Primary weight in evaluating these proposals is given to the general experience and specific project solutions provided by the Proposer. These components are found in the Technical Response & Evaluation Guide, RFQ Attachments A-C referenced above. Technical scores will include consideration of the oral presentations.
- 5.2.3 Cost proposals for each proposer within the Competitive Range will be opened and scored and the state will proceed with possible cost negotiations as applicable. The contract will be awarded to the qualified proposer with the highest combined scoring for technical and cost proposals.

Phase I: The State will evaluate the Mandatory Requirements set forth in RFQ Attachment A on a pass/fail basis.

Phase II: Following the Stage I evaluation, the State will apply a standard equitable evaluation model, which will represent a qualitative assessment of each response. Each response will be scored by Evaluation Team members according to the Technical Response & Evaluation Guides (See RFQ Attachments B & C).

The Solicitation Coordinator will total the average score from the evaluation team for each responsive and responsible Respondent's Technical Response Points for RFQ Attachments B & C to determine which of the Respondents are considered Qualified and within the competitive range.

The State may invite those who passed the Phase I evaluation to give oral presentations to the State. The qualitative assessment of each Respondent will include the information derived from the oral presentations.

**5.3 Cost Proposals:** Only Qualified Respondents that are responsive and responsible and in the competitive range will continue onto Stage Two, Cost Proposal evaluation. The Cost Proposal containing the lowest cost will receive the maximum number of points per each section. See RFQ Attachment D, Cost Proposal & Evaluation Guide and RFQ Attachment D.1, Cost Proposal Workbook.

**5.4 Clarifications and Negotiations:** The State reserves the right to award a contract on the basis of initial responses received; therefore, each response should contain the respondent's best terms from a technical and cost standpoint. However, the State reserves the right to conduct clarifications or negotiations with respondents. All communications, clarifications, and negotiations shall be conducted in a manner that supports fairness in response improvement.

5.4.1 Clarifications: The State may identify areas of a response that may require further clarification or areas in which it is apparent that there may have been miscommunications or misunderstandings as to the State's specifications or requirements. The State may seek to clarify those issues identified during one or multiple clarification round(s). Each clarification sought by the State may be unique to an individual respondent.

5.4.2 Negotiations: The State may elect to negotiate with Qualified Respondents, within the competitive range, by requesting revised responses, negotiating costs, or finalizing contract terms and conditions. The State reserves the right to conduct multiple negotiation rounds

5.4.2.1 **Cost Negotiations:** All Qualified Respondents within the competitive range will be given equivalent information with respect to cost negotiations. All cost negotiations will be documented for the procurement file. Additionally, the State may conduct target pricing and other goods or services level negotiations. Target pricing may be based on considerations such as current pricing, market considerations, benchmarks, budget availability, or other methods that do not reveal individual respondent pricing. During target price negotiations, respondents are not obligated to meet or beat target prices, but will not be allowed to increase prices.

5.4.2.2 If the State determines costs and contract finalization discussions and negotiations are not productive, the State reserves the right to bypass the apparent best evaluated Respondent and enter into contract negotiations with the next apparent best evaluated Respondent.

## 5.5 Evaluation Guide

The State will consider qualifications, experience, technical approach, and cost (if applicable) in the evaluation of responses and award points in each of the categories detailed below. The maximum evaluation points possible for each category are detailed below.

Evaluation Category	Maximum Points Possible
<b>Mandatory Requirement Items(refer to RFQ Attachment A)</b>	Pass/Fail
<b>General Qualifications &amp; Experience Items(refer to RFQ Attachment B)</b>	250
<b>Technical Qualifications, Experience &amp; Approach Items (refer to RFQ Attachment C)</b>	650
<b>Cost Proposal (refer to RFQ Attachment D and RFQ Attachment D.1)</b>	100

## 5.6 Contract Award

- 5.6.1 The Solicitation Coordinator will submit the Evaluation Team determinations and response scores to the head of the contracting agency, or the agency head's designee, for consideration along with any other relevant information that might be available and pertinent to contract award.
- 5.6.2 The contracting agency head, or the agency head's designee, will determine the apparent best-evaluated response. (To effect a contract award to a Respondent other than the one receiving the highest evaluation score, the head of the contracting agency must provide written justification and obtain written approval of the Chief Procurement Officer and the Comptroller of the Treasury.)
- 5.6.3 The State reserves the right to make an award without further discussion of any response.
- 5.6.4 The State will issue an Evaluation Notice and make the RFQ files available for public inspection at the time and date specified in the RFQ §2, Schedule of Events.

**NOTICE:** The Evaluation Notice shall not create rights, interests, or claims of entitlement in either the Respondent identified as the apparent best evaluated or any other Respondent.

- 5.6.5 The Respondent identified as offering the apparent best-evaluated must sign a contract drawn by the State pursuant to this RFQ. The contract shall be substantially the same as the RFQ Attachment G, pro forma Contract. The Respondent must sign said contract no later than the Respondent Contract Signature Deadline detailed in RFQ § 2, Schedule of Events. If the Respondent fails to provide the signed contract by the deadline, the State may determine the Respondent is non-responsive to this RFQ and reject the response.
- 5.6.6 Notwithstanding the foregoing, the State may, at its sole discretion, entertain limited negotiation prior to contract signing and, as a result, revise the pro forma contract terms and conditions or performance requirements in the State's best interests, PROVIDED THAT such revision of terms and conditions or performance requirements shall NOT materially affect the basis of response evaluation or negatively impact the competitive nature of the RFQ and vendor selection process.
- 5.6.7 If the State determines that a response is nonresponsive and rejects it after opening Cost Proposals, the Solicitation Coordinator will re-calculate scores for each remaining responsive Cost Proposal to determine (or re-determine) the apparent best-evaluated response.

## RFQ ATTACHMENT A

**TECHNICAL RESPONSE & EVALUATION GUIDE**

All Respondents must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). All Respondents must also detail the response page number for each item in the appropriate space below.

The Solicitation Coordinator will review all responses to determine if the Mandatory Requirement Items are addressed as required and mark each with pass or fail. For each item that is not addressed as required, the Evaluation Team must review the responses and attach a written determination. In addition to the Mandatory Requirement Items, the Solicitation Coordinator will review each response for compliance with all RFQ requirements.

<b>RESPONDENT LEGAL ENTITY NAME:</b>			
<b>Response Page # (Respondent completes)</b>	<b>Item Ref.</b>	<b>Section A – Mandatory Requirement Items</b>	<b>Pass/Fail</b>
		The Technical Response must be delivered to the State no later than the Technical Response Deadline specified in the RFQ § 2, Schedule of Events.	
		The Technical Response must not contain cost or pricing information of any type.	
		The Technical Response must not contain any restrictions of the rights of the State or other qualification of the response.	
		A Respondent must not submit alternate responses.	
		A Respondent must not submit multiple responses in different forms (as a prime and a subcontractor).	
	A1.	Provide the Statement of Certifications and Assurances (RFQ Attachment E) completed and signed by an individual empowered to bind the Respondent to the provisions of this RFQ and any resulting contract. The document must be signed without exception or qualification.	
	A2.	Provide a statement, based upon reasonable inquiry, of whether the Respondent or any individual who shall perform work under the contract has a possible conflict of interest (e.g., employment by the State of Tennessee) and, if so, the nature of that conflict.  NOTE: Any questions regarding the existence of conflict of interest shall be solely resolved within the discretion of the State, and the State reserves the right to cancel any award.	
	A3.	Provide a current bank reference indicating that the Respondent's business relationship with the financial institution is in positive standing. Such reference must be written in the form of a standard business letter, signed, and dated within the past three (3) months.	
	A4.	Provide two current positive credit references from vendors with which the Respondent has done business written in the form of standard business letters, signed, and dated within	

RESPONDENT LEGAL ENTITY NAME:		
		the past three (3) months.
A5.		Provide an official document or letter from an accredited credit bureau, verified and dated within the last three (3) months and indicating a positive credit rating for the Respondent (NOTE: A credit bureau report number without the full report is insufficient and will <u>not</u> be considered responsive.)
A6.		Provide written confirmation that the Proposer understands and agrees to comply with the State's Technology Architecture requirements as detailed in <a href="#">State of Tennessee Enterprise Technology Architecture documentation</a> (See RFQ Attachment H). (NOTE: Bidder's may propose technologies that do not align with the State of Tennessee Enterprise Technology Architecture.)
A7.		Provide written attestation that the Respondent does attest, certify, warrant, and assure that the Contractor shall not knowingly employ in the performance of this Contract employees who have been excluded from participation in the Medicare, Medicaid, and/or State CHIP programs pursuant to Sections 1128 of the Social Security Act.
A8.		Respondent must provide written attestation that the Proposer <u>has</u> successfully implemented, with minimal mitigation, at least two (2) large scale implementations which must be post-PPACA (Patient Protection and Affordable Care Act) Medicaid eligibility determination systems. Both implementations must meet all the following criteria: <ul style="list-style-type: none"> <li>a) Comparable in size and complexity to that specified herein, or larger; specifically the implementation must have included the following components 1) a rules based MAGI engine, 2) an application intake/processing function and 3) electronic content management functionality. In addition, the system must have serviced a population of at least 500,000 enrollees per year.</li> <li>b) Within the last five (5) years;</li> <li>c) For a state or local government health/human services agency;</li> <li>d) Included in the references;</li> <li>e) Performed as the prime contractor.</li> <li>f) Supporting documentation shall consist at a minimum of name of the entity, total contract value as set for the initial contract scope of work, number of enrollees, dates of the project, services provided by the proposer, project status as of RFQ proposal submission (e.g. complete, in progress), products implemented, and the modules/functionality within those products that were deployed.</li> </ul>
A9.		Respondent must provide written attestation that business rules engine included in the Proposer's Solution has been successfully implemented and is operational in at least two (2) other states. Identify the state(s).

**RESPONDENT LEGAL ENTITY NAME:**

**State Use – RFQ Coordinator Signature, Printed Name & Date:**

## RFQ ATTACHMENT B

## TECHNICAL RESPONSE & EVALUATION GUIDE

**SECTION B: GENERAL QUALIFICATIONS & EXPERIENCE.** The Respondent must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). The Respondent must also detail the response page number for each item in the appropriate space below. Evaluation Team members will independently evaluate and assign one score for all responses to General Qualifications & Experience Items.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	Item Ref.	Section B – General Qualifications & Experience Items
	B1.	Detail the name, e-mail address, mailing address, telephone number, and facsimile number of the person the State should contact regarding the response.
	B2.	Describe the Respondent's form of business ( <i>i.e.</i> , individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and business location (physical location or domicile).
	B3.	Detail the number of years the Respondent has been in business.
	B4.	Briefly describe how long the Respondent has been providing the goods or services required by this RFQ.
	B5.	Describe the Respondent's number of employees, client base, and location of offices.
	B6.	Provide a statement of whether there have been any mergers, acquisitions, or sales of the Respondent within the last ten (10) years. If so, include an explanation providing relevant details.
	B7.	Provide a statement of whether the Respondent or, to the Respondent's knowledge, any of the Respondent's employees, agents, independent contractors, or subcontractors, proposed to provide work on a contract pursuant to this RFQ, have been convicted of, pled guilty to, or pled <i>nolo contendere</i> to any felony. If so, include an explanation providing relevant details.
	B8.	Provide a statement of whether, in the last ten (10) years, the Respondent has filed (or had filed against it) any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors. If so, include an explanation providing relevant details.
	B9.	Provide a statement of whether there is any material, pending litigation against the Respondent that the Respondent should reasonably believe could adversely affect its ability to meet contract requirements pursuant to this RFQ or is likely to have a material adverse effect on the Respondent's financial condition. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it would impair the Respondent's performance in a contract pursuant to this RFQ.  NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.

RESPONDENT LEGAL ENTITY NAME:		
	B10.	<p>Provide a statement of whether there is any pending or in progress Securities Exchange Commission investigations involving the Respondent. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it will impair the Respondent's performance in a contract pursuant to this RFQ.</p> <p>NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders such opinions.</p>
	B11.	<p>Provide a brief, descriptive statement, not to exceed 15 pages, detailing evidence of the Respondent's ability to deliver the goods or services sought under this RFQ (e.g., prior experience, training, certifications, resources, program and quality management systems, etc.).</p>
	B12.	<p>Provide a narrative description, not to exceed 15 pages, of the proposed contract team, its members, and organizational structure along with an organizational chart identifying the key people who will be assigned to provide the goods or services required by this RFQ, illustrating the lines of authority, and designating the individual responsible for the completion of each task and deliverable of the RFQ.</p>
	B13.	<p>Provide a personnel roster listing the names of Key Personnel (as defined in RFQ Attachment G Section A.22.15 that the Respondent will assign to perform tasks required by this RFQ along with the estimated number of hours that each individual will devote to the required tasks. Follow the personnel roster with a resume for each of the people listed. The resumes must detail the individual's title, education, current position with the Respondent, and employment history in the appendix. All Key Personnel must have at least three (3) client references from projects of similar scope and size and for similar roles, within the last 5 years.</p>
	B14.	<p>Provide a statement of whether the Respondent intends to use subcontractors to accomplish the work required by this RFQ, and if so, detail:</p> <ol style="list-style-type: none"> <li>a) the names of the subcontractors along with the contact person, mailing address, telephone number, and e-mail address for each;</li> <li>b) a description of the scope and portions of the work each subcontractor will perform; <u>and</u></li> <li>c) a statement specifying that each proposed subcontractor has expressly assented to being proposed as a subcontractor in the Respondent's response to this RFQ.</li> </ol>
	B15.	<p>Provide documentation of the Respondent's commitment to diversity as represented by the following:</p> <ol style="list-style-type: none"> <li>a) <u>Business Strategy</u> Provide a description of the Respondent's existing programs and procedures designed to encourage and foster commerce with business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises. Please also include a list of the Respondent's certifications as a diversity business, if applicable.</li> <li>b) <u>Business Relationships</u> Provide a listing of the Respondent's current contracts with business enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises. Please include the following information: <ol style="list-style-type: none"> <li>1. contract description;</li> <li>2. contractor name and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled); and</li> <li>3. Contractor contact name and telephone number.</li> </ol> </li> </ol>

RESPONDENT LEGAL ENTITY NAME:		
		<p>c) <u>Estimated Participation</u> Provide an estimated level of participation by business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises if a contract is awarded to the Respondent pursuant to this RFQ. Please include the following information:</p> <ol style="list-style-type: none"> <li>1. a percentage (%) indicating the participation estimate. (Express the estimated participation number as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics only and <b>DO NOT INCLUDE DOLLAR AMOUNTS</b>);</li> <li>2. anticipated goods or services contract descriptions;</li> <li>3. names and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veterans) of anticipated subcontractors and supply contractors.</li> </ol> <p>NOTE: In order to claim status as a Diversity Business Enterprise under this contract, businesses must be certified by the Governor's Office of Diversity Business Enterprise (Go-DBE). Please visit the Go-DBE website at <a href="https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&amp;XID=9810">https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&amp;XID=9810</a> for more information.</p> <p>d) <u>Workforce</u>. Provide the percentage of the Respondent's total current employees by ethnicity and gender.</p> <p>NOTE: Respondents that demonstrate a commitment to diversity will advance State efforts to expand opportunity to do business with the State as contractors and subcontractors. Response evaluations will recognize the positive qualifications and experience of a Respondent that does business with enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises and who offer a diverse workforce.</p>
	B16.	<p>Provide a statement of whether or not the Respondent has any current contracts with the State of Tennessee or has completed any contracts with the State of Tennessee within the previous five-year period. If so, provide the following information for all current and completed contracts:</p> <ol style="list-style-type: none"> <li>a) the name, title, telephone number and e-mail address of the State contact responsible for the contract at issue;</li> <li>b) the name of the procuring State agency;</li> <li>c) a brief description of the contract's specification for goods or scope of services;</li> <li>d) the contract term; and</li> <li>e) the contract number.</li> </ol> <p>NOTES: Current or prior contracts with the State are <u>not</u> a prerequisite and are <u>not</u> required for the maximum evaluation score, and the existence of such contracts with the State will <u>not</u> automatically result in the addition or deduction of evaluation points.</p> <p>Each evaluator will generally consider the results of inquiries by the State regarding all contracts responsive to this item.</p>
	B17.	<p>Provide customer references from individuals who are not current or former State employees for projects similar to the goods or services sought under this RFQ and which represent:</p> <ol style="list-style-type: none"> <li>a) two (2) accounts Respondent currently services that are similar in size to the State; <u>and</u></li> <li>b) three (3) completed projects.</li> </ol> <p>References from at least three (3) different individuals are required to satisfy the requirements above, e.g., an individual may provide a reference about a</p>

RESPONDENT LEGAL ENTITY NAME:		
		<p>completed project and another reference about a currently serviced account. Respondent must include references from each of the qualifications specified in RFQ Attachment A, item A.8.</p> <p>The standard reference questionnaire, which <u>must</u> be used and completed, is provided at RFQ Attachment F. References that are not completed as required may be deemed nonresponsive and may not be considered.</p> <p>The Respondent will be <u>solely</u> responsible for obtaining fully completed reference questionnaires and including them in the sealed Technical Response. In order to obtain and submit the completed reference questionnaires, follow the process below:</p> <ol style="list-style-type: none"> <li>a) Add the Respondent's name to the standard reference questionnaire at RFQ Attachment F, and make a copy for each reference.</li> <li>b) Send a reference questionnaire and a new, standard #10 envelope to each reference.</li> <li>c) Instruct the reference to: <ol style="list-style-type: none"> <li>1. complete the reference questionnaire;</li> <li>2. sign <u>and</u> date the completed reference questionnaire;</li> <li>3. seal the completed, signed, and dated reference questionnaire within the envelope provided;</li> <li>4. sign his or her name in ink across the sealed portion of the envelope; and</li> <li>5. return the sealed envelope directly to the Respondent (the Respondent may wish to give each reference a deadline, such that the Respondent will be able to collect all required references in time to include them within the sealed Technical Response).</li> </ol> </li> <li>d) Do NOT open the sealed references upon receipt.</li> <li>e) Enclose all <u>sealed</u> reference envelopes within a larger, labeled envelope for inclusion in the Technical Response as required.</li> </ol> <p>NOTES: The State will not accept late references or references submitted by any means other than that which is described above, and each reference questionnaire submitted must be completed as required.</p> <p>The State will not review more than the number of required references indicated above.</p> <p>While the State will base its reference check on the contents of the sealed reference envelopes included in the Technical Response package, the State reserves the right to confirm and clarify information detailed in the completed reference questionnaires, and may consider clarification responses in the evaluation of references.</p> <p>The State is under <u>no</u> obligation to clarify any reference information.</p>
	B18.	<p>Provide a statement and any relevant details addressing whether the Respondent is any of the following:</p> <ol style="list-style-type: none"> <li>a) is presently debarred, suspended, proposed for debarment, or voluntarily excluded from covered transactions by any federal or state department or agency;</li> <li>b) has within the past three (3) years, been convicted of, or had a civil judgment rendered against the contracting party from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;</li> </ol>

<b>RESPONDENT LEGAL ENTITY NAME:</b>		
		<ul style="list-style-type: none"> <li>c) is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed above; and</li> <li>d) has within a three (3) year period preceding the contract had one or more public transactions (federal, state, local) terminated for cause or default. If Respondent has had a contract terminated for cause or default, provide information on the reason for contract termination.</li> </ul>
	B19.	<p>Provide a full listing of:</p> <ul style="list-style-type: none"> <li>a) Any liquidated damages paid and their triggering events; and</li> <li>b) Terminated contracts (mutually or otherwise) with any other public transactions (federal, state, local, or territories) within the last five (5) years.</li> </ul>
	B20.	<p>Explain if the proposed Solution or a portion thereof is in implementation or full production operation in another state. If in implementation, identify the state, the functions being implemented, and the planned implementation date. If in production, identify the state where the proposed Solution is in production, how long it has been in production, and the functions that are in production. For each Solution described, list the programs covered (e.g., Medicaid) and if the scope covers functions necessitated by the program listing in RFQ Attachment I. Please list the components from other states that you plan to reuse in your proposed Solution.</p>
	B21.	<p>The State is amenable to considering changes to RFQ Attachment G, pro forma contract. The State will take all reasonable suggested alternative or supplemental contract language changes by Respondents under advisement during the evaluation and post award processes, subject to any mandates or restrictions imposed on the State by applicable state or federal law. The State recommends that Respondents include with their technical response any alternative or supplemental suggested contract language that Respondents would like the State to consider. However, the State reserves the right, in its sole discretion, to reject any and all such proposed changes to the pro forma contract.</p> <p>Clearly indicate, by providing a "red-line" of RFQ Attachment G, pro forma contract, all suggested alternative or supplemental contract language. Do not include any exceptions or changes that (1) contradict a Federal requirement or a Mandatory Requirement, or (2) push back any deadlines.</p>
<b>SCORE (for <u>all</u> Section B—Qualifications &amp; Experience Items above)</b>		
<b>State Use – Evaluator Identification:</b>		

## RFQ ATTACHMENT C

**TECHNICAL RESPONSE & EVALUATION GUIDE**

**SECTION C: TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH.** The Respondent should explain its approach to providing goods or services to the State. The items listed below represent specific questions the State would request you answer in your response. For ease of review, please annotate your explanation so that it contains references to the items listed below where they are addressed. Respondent should not feel constrained to answer only the specific questions listed below in its explanation and should feel free to provide attachments if necessary in an effort to provide a more thorough response. Response to RFQ Attachment C not to exceed 300 pages (single sided page, minimum 10 point font, single line spacing, with one inch margins), excluding Requirements Traceability Matrix responses, and Microsoft Project Plan.

The Evaluation Team, made up of three (3) or more State employees, will independently evaluate and score the response to each item. Each evaluator will use the following whole number, raw point scale for scoring each item:

0 = little value 1 = poor 2 = fair 3 = satisfactory 4 = good 5 = excellent

The Solicitation Coordinator will multiply the Item Score by the associated Evaluation Factor (indicating the relative emphasis of the item in the overall evaluation). The resulting product will be the item's raw, weighted score for purposes of calculating the section scores as indicated.

<b>RESPONDENT LEGAL ENTITY NAME:</b>					
<b>Response Page # (Respondent completes)</b>	<b>Item Ref.</b>	<b>Section C— Technical Qualifications, Experience &amp; Approach Items</b>	<b>Item Score</b>	<b>Evaluation Factor</b>	<b>Raw Weighted Score</b>
	C.1.	Executive Summary – Please provide a summary of your response to this RFQ. The Executive Summary should describe the Respondent's understanding of the State's vision and objectives, as well as highlight key themes and components of the Respondent's response.		15	
	C.2.	Project Management and Governance Approach – The Respondent should detail its proposed approach to managing and governing the Eligibility Modernization Project (EMP). Specifically address the requirements in pro forma Contract (RFQ Attachment G) Sections a) A.7 Enterprise and Solution Architecture Alignment b) A.8 Project Management c) A.10.1 Gate Review		50	
	C.3.	Release Plan and Solution Approach – Describe the Solution and approach to implementation in order to meet the State's		30	

RESPONDENT LEGAL ENTITY NAME:				
		<p>vision and requirements. Specifically address the requirements in pro forma Contract (RFQ Attachment G) Sections</p> <ul style="list-style-type: none"> <li>a) A.6 Release Plan and Project Roadmap</li> <li>b) A.9 Solution Infrastructure</li> <li>c) A.13 Environments</li> </ul> <p>For this response please identify any software licenses and hardware required by the Solution. For reference, the State's proposed project phasing and other relevant information can be found in RFQ Attachment I. Provide a Microsoft Project Plan displaying the proposed project schedule by the proposed release date, deliverable, SDLC activities, and timings of each Gate Review.</p> <p>In the discussion of the Solution approach, pay particular attention to identifying portions of the Solution that will be reused from other states (and identify the states where they are currently used).</p>		
	C.4.	<p>Organizational Change Management and Training (OCMT) – Describe the Respondent's approach for supporting the OCMT process. Please pay particular attention to how training content or other documentation will be linked to/associated with Solution pages. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Sections:</p> <ul style="list-style-type: none"> <li>a) A.10.2 Stakeholder Analysis and Management</li> <li>b) A.20 OCMT</li> </ul>		30
	C.5.	<p>Business Analysis/Requirements Management – Describe the Respondent's approach to stakeholder analysis and requirements management. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Sections:</p> <ul style="list-style-type: none"> <li>a) A.10.3 Business Analysis Management</li> <li>b) A.10.9 Requirements Management</li> </ul>		30
	C.6.	<p>Business Process Management (BPM) – Describe the Respondent's approach to business process analysis, documentation, and execution. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.10.7.</p>		15
	C.7.	<p>Business Rules Management – Describe the Respondent's approach to business rules analysis, documentation, and execution and traceability. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.10.8.</p>		40

RESPONDENT LEGAL ENTITY NAME:					
	C.8.	Testing/Go Live – Describe the Respondent’s approach to test development, test management, beta testing and determinations of operational readiness. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Sections a) A.10.10 Test Management b) A.15 Operational Readiness c) A.16 Beta Test d) A.10.12 Integrated System Implementation Management		70	
	C.9.	Interface/Integration Management– Describe the Respondent’s approach to interface and integration management. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.10.11.		60	
	C.10.	Approach to Deliverables – Describe the Respondent’s approach to meeting the State’s requirements for deliverable submission and the required deliverables. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Sections: a) A.11 Deliverable Submission Process b) A.27 Table of Deliverables		30	
	C.11.	Data Conversion – Describe the Respondent’s approach to converting historical and administrative data from legacy system data sources to the Solution. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.14.		30	
	C.12.	Operations and Maintenance–Describe the Respondent’s approach to operating and maintaining the implemented Solution. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.17.		70	
	C.13.	Turnover – Describe the Respondent’s approach to transitioning TEDS Operations and Maintenance (O&M) to the State or Other State Contractors. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.18.		15	
	C.14.	Security and Privacy – Describe the Respondent’s approach to meeting the Security and Privacy requirements. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.19.		70	
	C.15.	Staffing – Describe the Respondent’s approach to staffing management. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Section A.22.		70	
	C.16.	Warranty/Post Implementation – Describe the Respondent’s approach to providing warranty		30	

RESPONDENT LEGAL ENTITY NAME:				
		and post implementation services. Specifically address the requirements in <i>pro forma</i> Contract (RFQ Attachment G) Sections: a) A.10.13 Post Implementation Evaluation b) A.26 Warranty		
	C.17.	Project Operations – The State has defined other requirements for the EMP Respondent. Describe the Respondent’s approach for meeting the requirements described in <i>pro forma</i> Contract (RFQ Attachment G) Sections: a) A.21 Quality Assurance and Monitoring b) A.23 Facility c) A.24 Status Performance Reporting.		15
	C.18.	Functional Requirements– Describe the Respondent’s approach of how TEDS will fulfil each of the functional requirements described in RFQ Attachment J. For this response, fully complete the workbook in RFQ Attachment J.1.		100
	C.19.	Non-Functional Requirements – Describe the Respondent’s approach of how TEDS will fulfil each of the non-functional requirements described in RFQ Attachment J. For this response, fully complete the workbook in RFQ Attachment J.2.		100
	C.20.	Effort Workbook – Describe the estimated effort, in resource hours, that the Respondent believes will be necessary to successfully implement the Solution in Tennessee. For this response, fully complete the workbook in RFQ Attachment K. Additional instructions are provided in the Excel Workbook. <b>Do not include pricing information of any kind.</b>		130
		<b><i>The Solicitation Coordinator will use this sum and the formula below to calculate the section score. All calculations will use and result in numbers rounded to two (2) places to the right of the decimal point.</i></b>	Total Raw Weighted Score: (sum of Raw Weighted Scores above)	
	Total Raw Weighted Score / Maximum Possible Raw Weighted Score (i.e., 5 x the sum of item weights above)		X 650 (maximum possible score)	= SCORE:
<b>State Use – Evaluator Identification:</b>				

**RESPONDENT LEGAL ENTITY NAME:**

***State Use – Solicitation Coordinator Signature, Printed Name & Date:***

**RFQ ATTACHMENT D****COST PROPOSAL & EVALUATION GUIDE**

The Cost Proposal table below and the Cost Proposal Excel spreadsheet contained in RFQ Attachment D.1 must be completed exactly as required and returned with the rest of the Contractor's response to this RFQ.

**NOTICE: THIS COST PROPOSAL MUST BE COMPLETED EXACTLY AS REQUIRED**

**COST PROPOSAL SCHEDULE**— The Cost Proposal, detailed below, shall indicate the proposed price for the delivery of specified goods for the entire scope of services including all services defined in the Scope of Services of the RFQ Attachment G, pro forma contract for the entire contract period. The Cost Proposal shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract resulting from this RFQ. All monetary amounts shall be in U.S. currency and limited to two (2) places to the right of the decimal point.

Respondents shall complete RFQ Attachment D.1, the Cost Proposal Excel spreadsheet. The Cost Proposal Excel spreadsheet contains cells for all proposed labor rates, hours, and assumptions for each stage of the project. Instructions for completing the Cost Proposal Excel spreadsheet are contained in worksheet 1, Instructions. Summary results from the Cost Proposal Excel spreadsheet, are entered into the summary Cost Proposal table below for purposes of Cost Proposal evaluation.

**NOTICE:** The Evaluation Factor associated with each line item of cost is for evaluation purposes only. The evaluation factors do NOT and should NOT be construed as any type of volume guarantee or minimum purchase quantity. The evaluation factors shall NOT create rights, interests, or claims of entitlement of the Respondent.

Notwithstanding the line item of costs herein, pursuant to the second paragraph of the pro forma contract section C.1 of RFQ Attachment G, "The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract."

This Cost Proposal must be signed, in the space below, by an individual empowered to bind the entity responding to the provisions of this RFQ and any contract awarded pursuant thereto. If said individual is not responding in an individual capacity or is not the President or Chief Executive Officer, this document must attach evidence showing the individual's authority to legally bind the entity responding to this RFQ.

<b>RESPONDENT SIGNATURE:</b>	
<b>PRINTED NAME &amp; TITLE:</b>	

<b>DATE:</b>	
--------------	--

<b>RESPONDENT LEGAL ENTITY NAME:</b>
--------------------------------------

Line item of cost Description	Proposed Cost	State Use Only	
		Evaluation Factor	Evaluation Cost (cost x factor)
I. Design, Development and Implementation (From Attachment D.1, Sheet 6, cell I22)	\$ _____	1	
II. Initial Operations (Sum of all O&M months during initial contract term; from Attachment D.1, Sheet 6, cell J22)	\$ _____	1	
III. Maintenance & Operations, YR-1 (From Attachment D.1, Sheet 6, cell H20)	\$ _____	1	
III. Maintenance & Operations, YR-2 (From Attachment D.1, Sheet 6, cell H20)	\$ _____	1	
III. Maintenance & Operations, YR-3 (From Attachment D.1, Sheet 6, cell H20)	\$ _____	1	
<b>EVALUATION COST AMOUNT</b> (sum of evaluation costs above):			
The RFQ Coordinator will use this sum and the formula below to calculate the Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.			
Lowest evaluation cost amount from <u>all</u> responses	x 100 (maximum section score)	=	
evaluation cost amount being evaluated		<b>SCORE:</b>	

State Use – RFQ Coordinator Signature, Printed Name & Date:

**RFQ ATTACHMENT E****STATEMENT OF CERTIFICATIONS AND ASSURANCES**

An individual responding in his or her individual capacity or legally empowered to contractually bind the Respondent must complete and sign the Statement of Certifications and Assurances below as required, and this signed statement must be included with the response as required by the Request for Qualifications.

The Respondent does, hereby, expressly affirm, declare, confirm, certify, and assure ALL of the following:

- a) The Respondent will comply with all of the provisions and requirements of the RFQ.
- b) The Respondent will provide all specified goods or services as required by the contract awarded pursuant to this RFQ.
- c) The Respondent accepts and agrees to all terms and conditions set out in the contract awarded pursuant to this RFQ.
- d) The Respondent acknowledges and agrees that a contract resulting from the RFQ shall incorporate, by reference, all Respondent responses as a part of the contract.
- e) The Respondent will comply, as applicable, with:
  - 1) the laws of the State of Tennessee;
  - 2) Title VI of the federal Civil Rights Act of 1964;
  - 3) Title IX of the federal Education Amendments Act of 1972;
  - 4) the Equal Employment Opportunity Act and the regulations issued thereunder by the federal government; and,
  - 5) the Americans with Disabilities Act of 1990 and the regulations issued thereunder by the federal government.
- f) To the best of the undersigned's knowledge, information or belief, the information detailed within the Response to the RFQ is accurate.
- g) The Response submitted to the RFQ was independently prepared, without collusion, and under penalty of perjury.
- h) No amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Respondent in connection with the request or any potential resulting contract.
- i) The Response submitted in response to the RFQ shall remain valid for at least 120 days subsequent to the date of the Response opening and thereafter in accordance with any contract pursuant to the RFQ.

By signature below, the signatory certifies legal authority to bind the responding entity to the provisions of this request and any contract awarded pursuant to it. The State may, at its sole discretion and at any time, require evidence documenting the signatory's authority to be personally bound or to legally bind the responding entity.

DO NOT SIGN THIS DOCUMENT IF YOU ARE NOT LEGALLY AUTHORIZED TO DO SO BY THE ENTITY RESPONDING TO THIS RFQ.

<b>SIGNATURE &amp; DATE:</b>	
<b>PRINTED NAME &amp; TITLE:</b>	
<b>LEGAL ENTITY NAME:</b>	
<b>FEIN or SSN:</b>	

**RFQ ATTACHMENT F****REFERENCE QUESTIONNAIRE**

The standard reference questionnaire provided on the following pages of this attachment **MUST** be completed by all individuals offering a reference for the Respondent.

The Respondent will be responsible for obtaining completed reference questionnaires as required (refer to RFQ Attachment B, General Qualifications & Experience Items, Item B17.), and for enclosing the sealed reference envelopes within the Respondent's Technical Proposal.

**REFERENCE QUESTIONNAIRE**

**REFERENCE SUBJECT:** RESPONDENT NAME (completed by Respondent before reference is requested)

The "reference subject" specified above, intends to submit a response to the State of Tennessee in response to the Request for Qualifications (RFQ) indicated. As a part of such response, the reference subject must include a number of completed and sealed reference questionnaires (using this form).

Each individual responding to this reference questionnaire is asked to follow these instructions:

- a) complete this questionnaire (either using the form provided or an exact duplicate of this document);
- b) sign and date the completed questionnaire;
- c) seal the completed, signed, and dated questionnaire in a new standard #10 envelope;
- d) sign in ink across the sealed portion of the envelope; and
- e) return the sealed envelope containing the completed questionnaire directly to the reference subject.

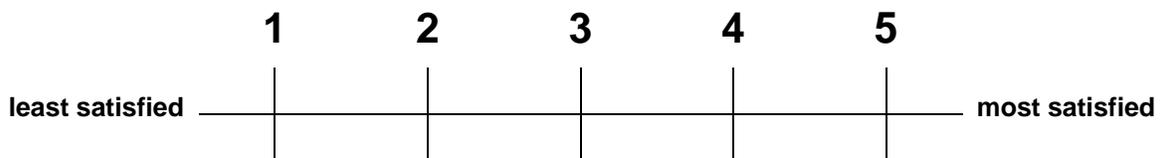
- 1) What is the name of the individual, company, organization, or entity responding to this reference questionnaire?
  
- 2) Please provide the following information about the individual completing this reference questionnaire on behalf of the above-named individual, company, organization, or entity.

<b>NAME:</b>	
<b>TITLE:</b>	

<b>TELEPHONE #</b>	
<b>E-MAIL ADDRESS:</b>	

- 3) What goods or services does/did the reference subject provide to your company or organization?
- 4) What is the level of your overall satisfaction with the reference subject as a vendor of the goods or services described above?

*Please respond by circling the appropriate number on the scale below.*



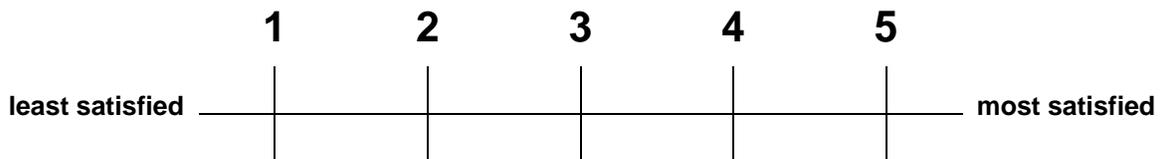
**If you circled 3 or less above, what could the reference subject have done to improve that rating?**

- 5) If the goods or services that the reference subject provided to your company or organization are completed, were the goods or services provided in compliance with the terms of the contract, on time, and within budget? If not, please explain.
- 6) If the reference subject is still providing goods or services to your company or organization, are these goods or services being provided in compliance with the terms of the contract, on time, and within budget? If not, please explain.
- 7) How satisfied are you with the reference subject's ability to perform based on your expectations and according to the contractual arrangements?
- 8) In what areas of goods or service delivery does/did the reference subject excel?

9) In what areas of goods or service delivery does/did the reference subject fall short?

10) What is the level of your satisfaction with the reference subject's project management structures, processes, and personnel?

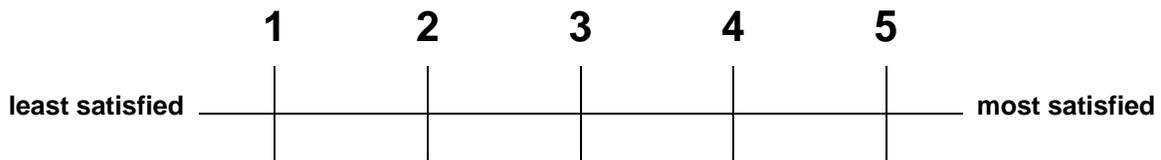
*Please respond by circling the appropriate number on the scale below.*



**What, if any, comments do you have regarding the score selected above?**

11) Considering the staff assigned by the reference subject to deliver the goods or services described in response to question 3 above, how satisfied are you with the technical abilities, professionalism, and interpersonal skills of the individuals assigned?

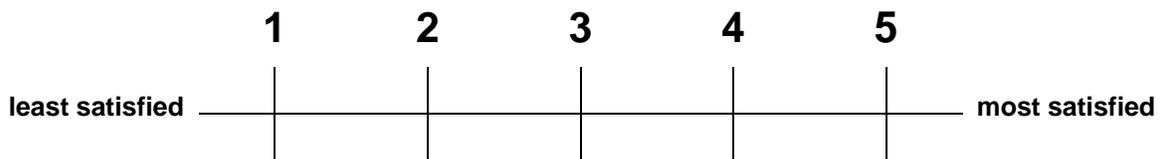
*Please respond by circling the appropriate number on the scale below.*



**What, if any, comments do you have regarding the score selected above?**

12) Would you contract again with the reference subject for the same or similar goods or services?

*Please respond by circling the appropriate number on the scale below.*



**What, if any, comments do you have regarding the score selected above?**

<p><b>REFERENCE SIGNATURE:</b> (by the individual completing this request for reference information)</p>	
--	--

<b>DATE:</b>	(must be the same as the signature across the envelope seal)
--------------	--

**PRO FORMA CONTRACT****RFQ # 32101-15557 PRO FORMA CONTRACT**

The pro forma contract detailed in following pages of this exhibit contains some "blanks" (signified by descriptions in capital letters) that will be completed with appropriate information in the final contract resulting from the RFQ.

**CONTRACT**

**BETWEEN THE STATE OF TENNESSEE,**

**DEPARTMENT OF FINANCE AND ADMINISTRATION,**

**DIVISION OF HEALTH CARE FINANCE AND ADMINISTRATION**

**AND**

**CONTRACTOR NAME**

This Contract, by and between the State of Tennessee, Department of Finance and Administration, Division of Health Care Finance and Administration (HCFA), hereinafter referred to as "HCFA" or the "State", and the Contractor, CONTRACTOR LEGAL ENTITY NAME, hereinafter referred to as the "Contractor", is for the provision of Systems Integration Services to support the State in completing the Eligibility Modernization Project, hereinafter referred to as "EMP," as further defined in the "SCOPE OF SERVICES." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is A/AN INDIVIDUAL, FOR-PROFIT CORPORATION, NON-PROFIT CORPORATION, SPECIAL PURPOSE CORPORATION OR ASSOCIATION, PARTNERSHIP, JOINT VENTURE, OR LIMITED LIABILITY COMPANY.

Contractor Edison Registration ID # Number

Contractor Place of Incorporation or Organization: LOCATION

**A SCOPE OF SERVICES**

- A.1 The Contractor shall provide all goods or services and deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.
- A.2 Nothing in this Contract shall be deemed to be a delegation to the Contractor of the State's non-delegable duties under the TennCare program administered by the single state agency, as designated by the State and the Centers for Medicare and Medicaid Services (CMS), pursuant to Title XIX of the Social Security Act (42 U.S.C § 1396 et seq.) and the Section 1115 research and demonstration waiver granted to the State and any successor programs, or the Federal Children's Health Insurance Program (CHIP), known in Tennessee as "CoverKids," administered by the State pursuant to Title XXI of the Social Security Act. Applicable Definitions and Abbreviations relative to this contract are located in Attachment 7.
- A.3 The descriptions of Contractor deliverables in this Contract do not include every possible duty, task, or intermediate deliverable necessary to achieve success on this Contract. The Contractor shall receive written approval by the State for deliverables requiring State approval to be effective. The Contractor understands and agrees that any perceived lack of detail in a specific area does not indicate that the Contractor will have no duties in that area. The Contractor shall fulfill the State's Contract goals and requirements in a cost-effective manner. This includes all intermediate steps, deliverables or processes reasonably necessary to achieve the desired outcome described in each Section of the Contract. Intermediate steps, processes or deliverables will be detailed in the Control Memorandum (CM), developed by the parties at the inception of each Gate Review of the Contract, using the CM process described in Section A.29 below.
- A.4 Tennessee Eligibility Determination System (TEDS or Solution) Overview

- A.4.1 The Contractor shall design, develop, implement, maintain and operate a rules-based Medicaid eligibility determination system that includes a:
    - A.4.1.1 Worker portal;
    - A.4.1.2 Member portal; and
    - A.4.1.3 Partner portal.
  - A.4.2 The Solution shall have the ability to perform the following activities, including but not limited to:
    - A.4.2.1 Determining eligibility automatically and without worker intervention when all eligibility criteria have been satisfied according to the State's Medicaid policies and Verification Plan.
    - A.4.2.2 Receiving application data
    - A.4.2.3 Performing member matching
    - A.4.2.4 Verifying eligibility data with Federal and State data sources
    - A.4.2.5 Determining MAGI and non-MAGI Medicaid eligibility and redetermination of eligibility,
    - A.4.2.6 Terminating or denying eligibility
    - A.4.2.7 Sending and receiving account transfers with the Federal Facilitated Marketplace
    - A.4.2.8 Providing Managed Care Organization selection
    - A.4.2.9 Sending and reconciling all necessary eligibility and enrollment information with other systems such as MMIS
    - A.4.2.10 Mailing or electronically mailing applicable notices and letters
    - A.4.2.11 Performing case maintenance activities and receiving complaints and requests for appeals.
  - A.4.3 The Contractor shall design, develop, implement, maintain and operate an electronic content management system to scan and store eligibility documents.
  - A.4.4 The Contractor shall demonstrate that the system is compliant with the CMS Seven Standards and Conditions guidelines as published in December 2015. The Contractor shall adhere to the CMS-defined critical success factors as documented in "EE CSF 2016-02-18".
  - A.4.5 The Contractor shall demonstrate that the system is compliant with the CMS Eligibility and Enrollment Supplement for MITA 3.0.
- A.5 Governance
- A.5.1 As part of the State's Medicaid Modernization Program (MMP), the State is implementing governance processes for IT-enabled transformation projects. The first iteration of the MMP Governance Framework was developed by the State's Technical Advisory Services

(TAS) Contractor and administered by the State's Strategic Program Management Office (SPMO) Contractor. It focuses on business and technical governance of the Eligibility Modernization Project (EMP). The Contractor shall be governed by the State's Governance Framework and participate in all Gate Reviews of this project where required by the State's Governance Framework as defined in the Program. The Contractor shall comply with the State's Governance Framework including:

- A.5.1.1 The Contractor shall fully participate in periodic oversight meetings and reviews with State personnel, the State's TAS, SPMO and Independent Validation and Verification (IV&V) contractors, and other internal and external stakeholders. Full participation includes, but is not limited to, making visible the status of Gate Review deliverables throughout the process, including in draft form.
  - A.5.1.2 The Contractor shall coordinate with the SPMO in its role as governance administrator and the IV&V contractor in its independent review role to facilitate the successful oversight of the Eligibility Modernization Project.
  - A.5.1.3 The Contractor shall comply with the latest version of applicable State of Tennessee and Federal Government policies and standards that govern EMP and SDLC processes.
  - A.5.1.4 The Contractor shall participate in governance training provided by the State.
  - A.5.1.5 The Contractor shall cooperate with the State's internal technical review boards (the Technical Architecture Review Board (TARB) and the Technical Change Control Board (TCCB)) to facilitate the successful oversight of the Operations and Maintenance phase of this project.
- A.6 Release Plan and Project Roadmap
- A.6.1 Contractor shall ensure that the Solution meets the State's schedule and release requirements. In building the Solution, Contractor shall comply with the requirements contained in this Contract, including but not limited to, those requirements contained in Contract Attachment TBD hereof. [CONTRACTOR'S NEGOTIATED RESPONSE TO Contract ATTACHMENT TBD]
- A.7 Enterprise and Solution Architecture Alignment
- A.7.1 . The Contractor shall align all Solution designs with the State's target system architecture and with the State's Enterprise Architecture Business Operating Model (EA-BOM) Management Plan. In addition, the Contractor shall meet the following requirements:
    - A.7.1.1 The Contractor shall adhere to architecture design standards as specified in the EA-BOM Management Plan.
    - A.7.1.2 The architecture design artifacts prepared by the Contractor shall adhere to architecture principles as established by the HCFA TARB.
    - A.7.1.3 The Contractor shall, as necessary and at no additional cost to the State, resolve any non-compliance of the Solution with the State's design standards. Exceptions may only be granted by the State's TARB in writing on a case by case basis.
    - A.7.1.4 The Contractor shall maintain solution architecture artifacts and design models in an industry standard Computer-Aided Software Engineering Tool. This includes

the ability to create new and maintain existing architecture artifacts. Contractor's design tool shall be interoperable with the State's design tool to facilitate import and export of enterprise and solution architecture artifacts between the State and the Contractor. The artifacts that must be maintained in a design tool include, but are not limited to, the models, matrices, and lists specified in the EA-BOM Management Plan.

- A.7.1.5 The Contractor shall keep the State continually informed of to the status of architecture artifacts as required during the SDLC through such means as reports, web pages, a query tool, etc.

## A.8 Project Management

- A.8.1 The Contractor shall develop a Project Management Plan (PMP), to be approved in writing by the State, upon start of work under this Contract. The PMP shall define the approach to managing delivery of Project Management Lifecycle (PMLC) Services on the EMP and shall be developed in alignment with industry standards in the Project Management Body of Knowledge (PMBOK) for program and project management, and the State's MMP PMP template.
  - A.8.1.1 The Contractor shall define Scope Management processes and procedures to ensure that all scope updates are escalated appropriately and addressed in a timely manner.
  - A.8.1.2 The Contractor shall define Communication Management processes and procedures to ensure that all relevant information is escalated appropriately and addressed in a timely manner.
  - A.8.1.3 The Contractor shall define Risk and Issue Escalation processes and procedures to ensure that important risks and issues are escalated appropriately and resolved in a timely manner.
  - A.8.1.4 The Contractor shall define Schedule Management processes and procedures to ensure that the project remains on schedule.
  - A.8.1.5 The Contractor shall define Quality Management processes and procedures to ensure continuous improvement.
  - A.8.1.6 The Contractor shall define Configuration Management processes and procedures to ensure all project artifacts can be tracked and identified throughout the project lifecycle.
  - A.8.1.7 The Contractor shall define Performance Management processes and procedures to ensure that goals are consistently being met in an effective and efficient manner.
  - A.8.1.8 The Contractor shall define Human Resource Management processes and procedures to onboard resources, provide appropriate training and orientation to the TEDS processes.
  - A.8.1.9 The Contractor shall define Financial Management processes and procedures to ensure budget tracking and earned value management.
- A.8.2 The Contractor shall create a baselined Project Plan within the PMP that shall be used to track project tasks, deliverables, milestones, dependencies, and resources to ensure

accurate project status reporting. The Contractor shall continuously update the Project Plan and provide the latest version to the State immediately upon request. The Contractor's Project Management Plan shall include tasks for the State and the State's Contractors as appropriate. In addition, Contractor shall develop and submit a Release Project Plan for every release. The Contractor's Project Plan for every release shall be approved in writing by the State. The Contractor's Project Plan milestones shall be integrated into the MMP Integrated Master Schedule (IMS) in coordination with the State's SPMO to provide a MMP-wide project schedule view.

- A.8.3 The Contractor shall adhere to the State's PMLC guidance. If issues, risks, or system defects are not addressed in a timely manner, or if system defects or errors persist or recur, the State reserves the right to require the Contractor to develop and execute a State approved Corrective Action Plan (CAP), as described in Section A.17.2.8. The State also reserves the right to mandate that the project management methodology be revised or that the processes and procedures necessary to meet any of the State required milestones or deliverables be altered, in order for completion of timely and quality project deliverables, and to eliminate or minimize negative affects to the EMP's success.
- A.8.4 The Contractor shall coordinate with the State and State Contractors, as defined as including the Strategic Program Management Office (SPMO), the Technical Advisory Services (TAS) team, and the Independent Verification and Validation (IV&V) team, as well as any other contractor to the State as deemed necessary to ensure the successful management of the Eligibility Modernization Project.

#### A.9 Solution Infrastructure

- A.9.1 The Contractor shall be responsible for developing and/or configuring the Solution to meet the needs of the State. This shall include building the system infrastructure for the Solution. The State of Tennessee Strategic Technology Solutions (STS) group within the Department of Finance and Administration shall provide secure hosting facilities and services for the Solution. The Contractor shall comply with all STS processes (e.g. the Build Book process), procedures, and standards. The implementation for the Solution includes two (2) data centers in Tennessee. The South Data Center is the primary hosting location in Smyrna, TN and the North Data Center is the secondary hosting located in Nashville, TN. A more distant hosting site may be selected and procured by HCFA IS to align with CMS guidance concerning geographic separation for Integrated Eligibility application disaster recovery site selection. The primary host site is also known as the production site, while the secondary site is planned to be used as a disaster recovery site. The Contractor shall work with the State to determine the disaster recovery hosting option.
- A.9.2 STS shall configure all of the network, server, and storage hardware at all State data centers up to the operating system level, under the direction of the Contractor and HCFA IS, to implement the Solution and supporting systems. The Contractor shall provide, in the timeframe defined by the project schedule, STS with the configuration specifications for the network, storage, virtual machines, hardware, and operating systems. The specifications include security hardening settings, under the direction of the Contractor and HCFA IS. STS provides patch management services for the operating system and underlying virtual hosting technology. The host hardware (e.g., servers), security devices (e.g., encryption devices, firewalls), routing devices (e.g., load balancers, switches), and communications link interfaces are provided and maintained by STS. This includes full rack configurations for all equipment; full rack uninterruptable power supplies, rack cooling, rack temperature and humidity sensors, and cable management. STS shall also provide connectivity within all State facilities and networks including the internet egress,

excluding such technologies specific to TEDS. The Contractor shall validate and verify that all of specifications have been met as documented.

- A.9.3 The Solution specific commercial off-the-shelf (COTS) software and applications shall be maintained by the Contractor for the duration of the Contract. All Operating System (OS), applications, and COTS software updates are coordinated between the State and all applicable State contractors via the Technical Change Control Board processes, as changes in one application may impact the Solution or other HCFA system operations. The COTS software versions and OS versions shall be maintained by the Contractor within one major version of the latest release unless explicitly waived in writing by the Technical Change Control Board.
- A.9.4 The Contractor shall use state approved tools and methodologies for maintaining oversight and control of the infrastructure build process. The Contractor shall be responsible for ensuring that the construction of the system infrastructure conforms to the requirements and design specifications contained in this Contract, including but not limited to, those described in Contract Attachment TBD [CONTRACTOR'S NEGOTIATED RESPONSE TO Contract ATTACHMENT TBD].

#### A.10 System Development Lifecycle (SDLC)

##### A.10.1 Gate Review

- A.10.1.1 The Contractor shall be responsible for all materials and presentations associated with the Gate Reviews in the CMS Information Technology Enterprise Lifecycle (IT ELC) System Development Lifecycle and any mandates made by CMS relative to the System Development Lifecycle.
- A.10.1.2 The Contractor shall participate in the Gate Review process.
- A.10.1.3 The Contractor shall produce all required documents and deliverables associated with each Gate Review and shall meet CMS Gate Review submission standards. As the passing of each Gate Review is of critical importance to continued federal funding and adherence to the anticipated implementation schedule, failure to pass a Gate Review shall be considered a material breach of this Contract. The State may initiate the Termination for Cause provisions located at Section D.6 in the event of such a Gate Review failure.
- A.10.1.4 The Contractor shall comply with the State's design reviews to ensure the technical fit of the design of the Eligibility Modernization Solution with Federal and State conditions and standards and that it is inter-operable with other Federal and State systems defined in the target system architecture for Eligibility Modernization.
- A.10.1.5 The Contractor shall participate in consultation with the State, CMS, TAS, SPMO, IV&V and other State Contractors or State entities as required to prepare for Gate Reviews.

##### A.10.2 Stakeholder Analysis and Management

- A.10.2.1 The Contractor shall work directly with assigned project Organizational Change Management and Training (OCMT) Team Members for any identified OCMT, Stakeholder, or Communication needs, as required by the State to ensure adherence with State-approved OCMT methodology.

- A.10.2.2 The Contractor shall assist the OCMT Team in assessing the EMP to initially define and/or refine OCMT scope and overall approach as inputs for the development of any stakeholder engagement plans.
- A.10.2.3 The Contractor shall work with the OCMT Team to identify appropriate stakeholders and messaging for project-related communication and engagement needs.
- A.10.2.4 The Contractor shall adhere to the OCMT MMP Stakeholder Management Plan(s) and follow relationship/interaction mapping requirements when identifying and/or engaging stakeholders for the purpose of data and information collection.
- A.10.2.5 The Contractor shall coordinate and communicate stakeholder engagement needs and results to the designated OCMT Stakeholder Register Manager.
- A.10.2.6 The Contractor shall coordinate with the State Project Director in compliance with communication plan(s) on all identified communication needs, to ensure any communication needs are in alignment with, and/or added to, the approved project-specific communication(s) plan as defined by the project team.
- A.10.2.7 The Contractor shall provide access to key documentation and subject matter experts in any quantity and quality as the State deems reasonable to support assessing organizational impact and other OCMT activities as needed.
- A.10.2.8 The Contractor shall provide the project plan and validate major milestones and timing, as requested to the state, to ensure alignment with Stakeholder and/or OCMT activities across the project lifecycle.
- A.10.2.9 The Contractor shall provide resources sufficient in any quantity and capability as deemed reasonable by the State to support the following OCMT Approach activities, including but not limited to:
  - A.10.2.9.1 All the activities defined to support the various phases of the OCMT Approach (Analysis, Design, Development, Test, Implementation, O&M, and Evaluate) and/or Stakeholder Analysis and Management Plan, both documents being defined by the State.
  - A.10.2.9.2 Proactively identifying or assisting in the identification of areas of impact and the potential resolution areas of impact as they pertain to organizational design requirements and applicable stakeholder engagement plans.
  - A.10.2.9.3 Supporting the identification of key stakeholders.
  - A.10.2.9.4 Validating identified change impacts (both system and process related).
  - A.10.2.9.5 Providing subject matter experts in specific work areas, processes, applications, etc. to support awareness building sessions and/or other stakeholder engagement activities.
- A.10.3 Business Analysis Management
  - A.10.3.1 The Contractor shall document its standards, methodologies, and tools for conducting business analysis within the Requirements Management Plan, and

demonstrate the alignment to industry standards as defined by the International Institute of Business Analysis.

- A.10.3.2 The Contractor shall identify the delivery schedule and frequency of requirement artifacts ((such as, but limited to, Business Requirements Document (BRD), System Design Document (SDD)).
  - A.10.3.3 The Contractor shall integrate its business analysis activities into the State Enterprise Architecture and enterprise governance processes.
  - A.10.3.4 The Contractor shall document its approach to ensure provision of qualified Business Analysts with appropriate Medicaid domain knowledge and Business Analyst experience.
- A.10.4 Refine/Elaborate requirements
- A.10.4.1 The Contractor shall identify the stakeholders necessary for participation in the business analysis and requirements gathering activities.
  - A.10.4.2 The Contractor shall review proposed requirements as documented by the State, identify gaps, identify necessary clarifications, and offer alternatives to support solution development.
  - A.10.4.3 The Contractor shall secure clarification from relevant business and technical Subject Matter Experts (SMEs) to resolve ambiguous or conflicting requirements.
  - A.10.4.4 The Contractor shall conduct requirements gathering and refinement sessions with appropriate State and State-designated business and technical stakeholders, following industry standards such as those articulated by the International Institute of Business Analysis and the Business Analysis Body of Knowledge (BABOK).
  - A.10.4.5 The Contractor shall document any refined requirements for State approval in the Requirements Traceability Matrix, while maintaining requirement version control and archiving.
  - A.10.4.6 The Contractor shall write any new or revised business requirements such that they are understandable to the business stakeholders and not technical in nature.
- A.10.5 Support Design
- A.10.5.1 The Contractor shall review the State Enterprise and Business Architecture to gain an understanding of the desired business processes for Medicaid eligibility determinations.
  - A.10.5.2 The Contractor shall provide a Business Case Document describing the analysis that was completed and the Contractor's Solution, and highlighting the benefits of moving forward with the Solution.
  - A.10.5.3 The Contractor shall ensure that all aspects of the system are analyzed for the use of industry standard practices, focusing at a minimum on:
    - a) Meeting the needs of the business in a safe and secure manner (including Access Management and threat vulnerability assessment);
    - b) Meeting the needs of external stakeholders (including, but not limited to,

residents of Tennessee, Medicaid applicants, State and Federal government agencies such as CMS, Internal Revenue Service, Social Security Administration, State of Tennessee Strategic Technical Services, State of Tennessee Department of Human Services, and other State-approved contractors);

- c) Ensuring State-approved approach for Business Continuity/Disaster Recovery (BC/DR).

#### A.10.6 Support Change Requests

- A.10.6.1 The Contractor shall review Business Services Definitions issued by CMS and provide the State with a solution impact analysis on requirements, business rules, and interfaces within seven (7) calendar days of receipt of change request.
- A.10.6.2 The Contractor shall perform impact analysis on change requests to identify impacts across business processes and business rules.
- A.10.6.3 The Contractor shall perform risk analysis on change requests to identify risks and potential mitigations associated with development and deployment of the change.
- A.10.6.4 The Contractor shall perform alternatives analysis for change requests, to support the Eligibility Modernization Project Steering Committee (Project Steering Committee) with relevant information concerning alternative approaches to addressing the business need underlying the request.
- A.10.6.5 The Contractor shall perform cost analysis for change requests as part of the Change Order process described in Section A.28. All change requests shall indicate implementation and full lifecycle costs for the proposed change.
- A.10.6.6 The Contractor shall work with State management to understand the impact of human resource costs as well as cross-project impacts associated with fulfilling the change request.
- A.10.6.7 The Contractor shall provide analysis to support timing decisions for deployment of change requests, in compliance with the State release management process.

#### A.10.7 Business Process Management (BPM)

- A.10.7.1 The Contractor shall develop, for State approval, a BPM Plan. The Contractor shall execute this plan. This plan shall include at a minimum:
  - A.10.7.1.1 The tools that the Contractor shall use for documenting and managing business processes.
  - A.10.7.1.2 The documentation standards that shall be used for business processes.
  - A.10.7.1.3 The process by which business processes shall be evaluated, for both new and revised processes.
  - A.10.7.1.4 The roles and responsibilities of the Contractor, the State, and other MMP Contractors in BPM for the project. This includes supporting the entire business process by defining, documenting, and proposing improvements to business process standards.

- A.10.7.2 The Contractor shall validate State future state business processes against the Solution and provide a gap and alternatives analysis.
- A.10.7.3 The Contractor shall ensure that the business processes, as documented, are in alignment with the State Business Architecture.
- A.10.7.4 The Contractor shall ensure that business processes are reviewed and approved by the State designated project stakeholders.
- A.10.7.5 The Contractor shall use industry-standard software in capturing the business processes end-to-end. Any such software shall at a minimum:
  - A.10.7.5.1 Capture all workflows, including workflows with human-to-human processes, human-to-system processes, and system-to-system processes.
  - A.10.7.5.2 Allow updates to be applied to workflows with minimal effort and allowing for the capture of the dynamic changes to the modified workflow and that demonstrates traceability between business processes and business requirements.
  - A.10.7.5.3 Provide process flow documentation, consistent with the standards outlined in Tennessee Business Solutions Methodology Business Process Description (found at <http://www.tn.gov/assets/entities/finance/attachments/TBSMBusinessProcessDescription.xlsx>) and the BABOK.
  - A.10.7.5.4 Maintain versions of business processes, beginning with a baseline or current version, and maintaining each version when updates are applied, including graphical representation of the same business processes.
  - A.10.7.5.5 Provide traceability of business processes to the Business Architecture and business rule(s) that apply to the documented process.
- A.10.7.6 The Contractor shall design a Solution that allows for execution of the business processes. Any such Solution shall, at a minimum:
  - A.10.7.6.1 Comply with and use, to the extent possible, technologies outlined in the Enterprise Architecture.
  - A.10.7.6.2 Comply with or include a Business Rules Engine (BRE) or Business Rules Management software for handling the business rules governing the processes.
  - A.10.7.6.3 Comply with documented enterprise and Business Architecture. The Contractor shall secure State written approval, through the appropriate State governance body, for any variance from the State architectural standards.
  - A.10.7.6.4 The Contractor shall ensure that the implementation is compatible with the Enterprise Architecture, and is approved in writing by the State as being able to meet the technical and business needs. The Contractor agrees and understands using a custom implementation that is not natively compatible with the Enterprise Architecture requires a State-approved exception.

- A.10.7.7 The Contractor shall document changes to the business processes that have been identified and approved by the State.
  - A.10.7.8 The Contractor shall ensure that the tool being used to manage business processes shall be able to identify and model the effects of the change to other business processes.
  - A.10.7.9 The Contractor shall work with the State to submit any proposed changes to a business process to the Project Steering Committee and other governance or review boards as designated by the Project Steering Committee.
  - A.10.7.10 The Contractor shall perform an impact analysis on any proposed changes to business processes. Such analysis shall include, at a minimum:
    - A.10.7.10.1 Cost implications of making the change
    - A.10.7.10.2 Security and privacy implications of the change
    - A.10.7.10.3 Identification of the impact of the change on related business processes
    - A.10.7.10.4 Identification of configuration changes needed based on the proposed change
    - A.10.7.10.5 Analysis of new business requirements against current requirements to ensure that any new requirements are not in conflict with current requirements
    - A.10.7.10.6 Identification of project risk implications associated with the proposed change
    - A.10.7.10.7 Identification of project assumptions and constraints associated with the proposed change.
  - A.10.7.11 The Contractor shall ensure that any proposed changes that may affect the Business or Enterprise Architecture shall be reviewed by the TARB for approval before implementation of the change.
  - A.10.7.12 The Contractor shall conduct an impact analysis, as needed, to support proposed or anticipated retirement of a business process or solution.
- A.10.8 Business Rules Management
- A.10.8.1 The Contractor shall develop a Business Rules Management Plan to include and execute on the following activities:
    - A.10.8.1.1 Identify an industry-recognized BRE or Business Rules Management System (BRMS) which the Contractor shall use to document business rules.
    - A.10.8.1.2 Provide the State a written justification describing the preferred BRE or BRMS solution and the selection process used to compare the preferred solution with other industry-recognized solutions.
    - A.10.8.1.3 Implement BRE or BRMS solution only after the State has given approval to use the preferred BRE or BRMS solution.

- A.10.8.1.4 Allow for execution of the business rules, as well as the ability for expert State business users to review and test the business rules.
  - A.10.8.1.5 Ensure that the implemented BRE or BRMS is compliant with the Minimum Acceptable Risk Standards for Exchanges (MARS-E), and properly aligned with the project Security Plan.
  - A.10.8.1.6 Define business rules documentation standards, subject to State approval, and consistent with CMS Seven Conditions and Standards.
  - A.10.8.1.7 Identify responsibilities for Business Rules Management, including critical access and segregation of duties considerations.
  - A.10.8.1.8 Review the BRD and obtain State approval for any changes made.
  - A.10.8.1.9 Demonstrate to the State that the implementation of any new business rules have not resulted in any circular errors or broken cases elsewhere.
- A.10.8.2 Define Business Rules Format:
- A.10.8.2.1 The Contractor shall ensure that the business rules contain a unique identifier for each rule.
  - A.10.8.2.2 The Contractor shall ensure that the business rules contain a description of the rule.
  - A.10.8.2.3 The Contractor shall ensure that business rules capture any relationship between other business rules and business requirements.
- A.10.8.3 Define Business Rules Standards:
- A.10.8.3.1 The Contractor shall separate business rules from core programming, as specified by the MITA Modularity Standard.
  - A.10.8.3.2 The Contractor shall write business rules as a clear directive or statement specific to one topic.
  - A.10.8.3.3 The Contractor shall write business rules that are understandable to the business owners and not technical in nature.
  - A.10.8.3.4 The Contractor shall provide business rules in human-and machine-readable format.
  - A.10.8.3.5 The Contractor shall engage appropriate State business Subject Matter Experts to assist the Contractor in writing the business rules.
  - A.10.8.3.6 The Contractor shall write business rules that convey what shall happen or what can only happen if a certain condition is met.
  - A.10.8.3.7 The Contractor shall provide a mechanism and a process to maintain business rules and regularly review for accuracy, updates, or retirement as necessary.
  - A.10.8.3.8 The Contractor submit all business rules to the State for their written approval.

#### A.10.8.4 Implementing Business Rules:

- A.10.8.4.1 The Contractor shall, as needed, conduct requirements analysis and secure requirements approval from the State for proposed changes to business rules.
- A.10.8.4.2 The Contractor shall, as needed, conduct design definition and review sessions to support a proposed update to business rules, and shall secure State approval for the proposed change.
- A.10.8.4.3 The Contractor shall submit updates to business rules as regulatory, business, functional, security, technology, or other factors dictate and shall secure State approval for the proposed change.
- A.10.8.4.4 The Contractor shall be responsible for providing all required supporting information, including cost and impact analysis, relative to proposed business rules changes for presentation to the Project Steering Committee and any other State architecture or governance review bodies as designated by the Project Steering Committee.
- A.10.8.4.5 The Contractor shall update the Requirements Traceability Matrix as needed to reflect any approved changes to requirements associated with the business rules, including changes to downstream requirements.
- A.10.8.4.6 The Contractor shall implement changes to business rules only upon State approval of the change, while maintaining business rules version control and archiving.
- A.10.8.4.7 The Contractor shall ensure that the Business Rule configuration items (CI) are updated and maintained.

#### A.10.8.5 Traceability within the System Development Lifecycle:

- A.10.8.5.1 The Contractor shall ensure bi-directional traceability between rule-related requirements and the associated business rules.
- A.10.8.5.2 The Contractor shall ensure that business requirements are inclusive of all business rules.
- A.10.8.5.3 The Contractor shall ensure that business rules are assessed against functional and non-functional requirements, as well as any proposed technical solutions or implementation.
- A.10.8.5.4 The Contractor shall ensure that designs are inclusive of all business rules.
- A.10.8.5.5 The Contractor shall document acceptance criteria approved by the State for all business rules to support test execution.
- A.10.8.5.6 The Contractor shall provide a test plan that includes testing the implementation against the constraints dictated by the business rules.
- A.10.8.5.7 The Contractor shall have in place a process to identify and track post-implementation defects between the implemented Solution and business rules as part of the software problem resolution process.

- A.10.8.5.8 The State shall be responsible for notifying the Contractor of any changes to business rules that are an outcome of policy changes.
- A.10.8.5.9 The Contractor shall have in place a process in which any changes to the business rules are reviewed by the State before being updated in the BRE or BRMS.
- A.10.8.5.10 The Contractor shall be responsible, through the Stakeholder Management Process, in notifying key stakeholders when business rules need to change based on a Project Steering Committee approval to make the change.

#### A.10.9 Requirements Management

- A.10.9.1 The Contractor shall be responsible for producing and executing a Requirements Management Plan, subject to State approval, that follows the State framework standard. The Requirements Management Plan shall
  - A.10.9.1.1 Describe the project's methodology for requirements that meet the State's standard.
  - A.10.9.1.2 Identify and maintain a list of stakeholders necessary for participation in the requirements lifecycle, clearly documenting their roles in the process.
  - A.10.9.1.3 Describe the performance measures, processes, and methods that shall be used by the Contractor to monitor and enforce compliance with requirements while maintaining quality requirements management throughout the project lifecycle.
  - A.10.9.1.4 Provide a process for the disciplined management of requirements across the requirements lifecycle, from ideation through implementation and retirement.
  - A.10.9.1.5 Include a detailed standard operating procedure manual for the definition, maintenance and change process for requirements in the Contractor's requirements management tool.

#### A.10.9.2 Requirements Definition & Management

- A.10.9.2.1 The Contractor shall incorporate State-defined requirements associated with the State's business operating model into the aggregate requirements documentation and requirements management tool.
- A.10.9.2.2 The Contractor shall be responsible for managing the review and approval process for newly identified business or Solution requirements, or the iteration of State-defined requirements through to the end of the requirements lifecycle.
- A.10.9.2.3 The Contractor shall be responsible for defining transition requirements in support of the designed Solution, as per the State standard, and subject to State approval.
- A.10.9.2.4 The Contractor shall be responsible for completing the following tasks during business, solution or transition requirements definition and management:

- a) The Contractor shall conduct necessary requirements gathering activities to document all requirements and associated requirement types to meet the State's needs and achieve CMS compliance.
- b) The Contractor shall engage all necessary stakeholders, including the State, Strategic Technology Services (STS), and other State-designated entities, in requirements definition activities, to support completeness of solution and transition requirements.
- c) The Contractor shall validate requirements with relevant State personnel to validate that requirements are well-defined, understood, and documented.
- d) The Contractor shall document requirements in a manner consistent with the CMS Business Requirements Writer's Guide.
- e) The Contractor shall document all requirements in a requirements document that aligns to the CMS and State Requirements Document template.
- f) The Contractor shall ensure that requirements specifications have been developed for all hardware and software subsystems in a sufficient level of detail to ensure successful implementation.
- g) The Contractor shall ensure that that all maintenance requirements for the system are completely specified.
- h) The Contractor shall elicit and document performance requirements (e.g. timing, response time and throughput) to satisfy user needs.
- i) The Contractor shall describe and document all system interfaces precisely, by interface protocol and by function, including input/output control codes, data format, polarity, range, units, and frequency.
- j) The Contractor shall identify and document known constraints or limitations early in the requirements gathering process.
- k) The Contractor shall ensure that the requirements at a minimum:
  - 1) Are uniquely identified throughout their lifecycle
  - 2) Include system calculations, data manipulation and processing, user interface and interaction with the application, and other specific functionality showing how user requirements shall be satisfied.
  - 3) Describe the existing technical environment, systems, functions, and processes.
  - 4) Describe hardware/software requirements that will limit the design and/or use of COTS options. These may include laws, regulations, hardware limitations, interfaces, development environment, operational environment, criticality, safety, and/or security.

- 5) Describe hardware requirements and any related processes. This shall include a detailed description of specific hardware requirements, associated to specific project functionality/deliverables, and shall include information such as type of hardware, brand name, specifications, size, and security, and other relevant characteristics.
- 6) Describe software requirements and any related processes. This shall include a detailed description of specific software requirements associated to specific project functionality/deliverables, and shall include all relevant information, such as security standards, version numbering, functionality, data, interface requirements, and specifications.
- 7) Describe performance requirements and any related processes, including a detailed description of specific performance requirements associated to specific project functionality/deliverables. This shall include information such as system capacity, cycle time, speed per transaction, test requirements, minimum defect counts, screen refresh rates, reliability, utilization and other criteria necessary to define performance and capacity.
- 8) Describe all of the Non-functional Requirements that affect availability, including hours of operation, level of availability required, down-time impact, support availability, accuracy, and any other criteria necessary to define availability.
- 9) Describe all of the non-functional requirements that affect supportability and maintainability such as coding standards, naming conventions, maintenance access, and required utilities.
- 10) Describe the requirements for any user documentation and help systems, including context-based application support.
- 11) Describe all of the user interface requirements (e.g., user navigation, presentation of application and associated functionality, screen location of interface elements, data display and manipulation), system interfaces, and hardware and software requirements that affect interfaces, protocol management, scheduling, directory services, broadcasts, message types, error and buffer management, and security.
- 12) Summarize and make reference to the Privacy Impact Assessment, as defined in Section A.27, and its impact on security requirements and provide justifications for why a specific privacy item is needed.
- 13) Provide security categorization if available and describe all of the non-functional requirements that affect security such as security audits, cryptography, user data, system identification/authentication, resource utilization, and facility access times.

- 14) Describe the existing compliance environment as it affects project requirements, and the standards that solution development must follow. Include an overview of the compliance or standards requirements necessary to achieve the project's objectives. List all that are applicable to the project.
- 15) Include a section that applies to the systems that are required to be Section 508 and WCAG 2.0 AA compliant and describes how Section 508 of the Rehabilitation Act and WCAG 2.0 AA affects the system, citing the technical standards it shall meet.
- i) The Contractor shall maintain all requirements under formal configuration control.
  - ii) The Contractor shall secure State approval of all baseline requirements.
  - iii) The Contractor shall make no changes to the requirement baseline except where the requirement change has been approved by the Project Steering Committee.
  - iv) The Contractor shall update project and test plans for any new requirements approved by the Project Steering Committee.
  - v) The Contractor shall document requirements to support traceability through design, build, and test to validate and verify that the system performs as intended and contains no unnecessary software elements.
  - vi) The Contractor shall provide a process for identifying, avoiding, and resolving conflicts or duplication of requirements and business rules.
  - vii) The Contractor shall identify testing or completion criteria for each requirement, subject to State review and approval.

#### A.10.9.3 Requirements Traceability & Requirements Management Tool

- A.10.9.3.1 The Contractor shall provide an industry standard Requirements Management tool, Test Management tool, and Business Rules Management tool.
- A.10.9.3.2 The Contractor shall be solely responsible for maintaining business, solution and transition requirements in an industry standard requirements management tool.
- A.10.9.3.3 The Contractor's Requirements Management tool must be interoperable with industry standard requirements management tools, the Contractor's Test Management tool, and the Contractor's Business Rules Management tool.

- A.10.9.3.4 The Contractor shall be able to demonstrate the traceability between requirements and solution design elements, business rules, data elements, architecture artifacts, and test cases as per the State's Requirements Management Plan standard, within the Contractor's toolsets. Traceability shall include the ability to trace business requirements to solution requirements, backward and forward traceability between solution requirements and other solution requirements, and solution requirements to transition requirements. Traceability shall also include solution requirement ordering to show dependencies between requirements.
- A.10.9.3.5 The Contractor shall give the State unrestricted access to the requirements management tool throughout the project SDLC.
- A.10.9.3.6 The Contractor shall ensure that individuals responsible for managing requirements are trained in the appropriate requirements management procedures and use of the project's requirement management tool.
- A.10.9.3.7 The Contractor shall use its requirements management and test management tool to trace requirements to test cases and results.
- A.10.9.3.8 The Contractor's requirements management tool at a minimum shall:
- a) Assign or allow for the assignment of a unique identifier to each requirement
  - b) Collect the source of the business requirement
  - c) Collect a title of the requirement
  - d) Collect the detailed description of the requirement
  - e) Collect the owner of the requirement
  - f) Collect any assumptions applied to the business requirement
  - g) Assign a date and user stamp for the requirement when created
  - h) Assign or allow for the assignment of the business requirement type (e.g., functional, non-functional, technical.)
  - i) Allow for reporting the current status of the business requirement in the lifecycle
  - j) Allow for identifying the business process(es) to which the requirement applies
  - k) Allow for the attachment or referencing of external documents related to the requirement
  - l) Have the ability to track changes made to the requirement in a way that allows for generating a historical view of the requirement, capturing when and by whom the change was made
  - m) Identify and demonstrate the relationship between requirements,

functional or otherwise; business rules; and artifacts that directly affect the requirement (e.g. process flows)

- n) Allow for hierarchical creation and sorting of requirements
- o) Provide a reporting mechanism that allows requirement reports to be generated based on:
  - 1) requirement status
  - 2) requirement type
  - 3) the hierarchy to which they are assigned, or
  - 4) the business process/architectural feature to which they relate

#### A.10.10 Test Management

- A.10.10.1 The Contractor shall be responsible for any and all testing required for building and implementing the TEDS.
- A.10.10.2 The Contractor shall provide test cases and scenarios for use by the State during user acceptance testing. The State shall have the ability to create additional test cases, as necessary.
- A.10.10.3 The Contractor's test cases shall cover interface performance in support of the eligibility determination process.
- A.10.10.4 The Contractor shall create and execute a Test Management Plan for State approval, prior to any release or approved configuration change that defines the testing methodology, the types of tests to be performed during the lifecycle, testing schedule, and how the testing functions shall be performed.
- A.10.10.5 The Contractor shall ensure that the Test Management Plan is in compliance with the CMS Testing Framework and adheres to the appropriate Gate Reviews as prescribed in this Framework.
- A.10.10.6 The Contractor shall ensure that the Test Management Plan is in compliance with security standards as set by the CMS Testing Framework, CMS Information Security Standards, and Acceptable Risk Safeguards, and the security standards included in this Contract.
- A.10.10.7 The Contractor shall ensure that the Test Management Plan appropriately addresses compliance with Minimum Acceptable Risk Standards for Exchanges (MARS-E), Social Security Administration (SSA), and Federal Tax Information (FTI) security requirements.
- A.10.10.8 The Test Management Plan shall conform to the standards outlined in the HCFA Test Management Plan and shall outline the Contractor's approach, methodology, and associated documentation for defining:
  - A.10.10.8.1 The scope of test work planned, partitioned into logical modules based on functional or other characteristics that shall provide an appropriate level of clarity for understanding and monitoring testing progress.

- A.10.10.8.2 The types of tests the Contractor shall use to test the release, which shall conform to the testing types designated by the CMS Testing Framework and the HCFA Test Management Plan.
  - A.10.10.8.3 The testing environments (hardware and software) required to support testing activities in a way that Testing and Development environments shall manage all data in compliance with State and Federal regulations and policies.
  - A.10.10.8.4 The strategy for addressing testing-related activities associated with Gate Reviews and providing State-approved test coverage, as applicable.
  - A.10.10.8.5 The strategy for use of State-approved testing tools that the Contractor shall use to perform all testing responsibilities, ensuring that such tools are available to complete full integration, security, performance, regression and stress testing in the appropriate environments.
  - A.10.10.8.6 The expected timeline for completing each test phase, including contingency plans (CP) if for any reason milestones become at risk for not being completed within the set timeline.
  - A.10.10.8.7 The testing sequence and frequency and the reporting recurrence for test results.
  - A.10.10.8.8 The assumptions, constraints, and risks involved with the testing activity, to include any mitigation plans, workarounds, or deferrals that have been approved by the State and taken into consideration during testing.
  - A.10.10.8.9 The Contractor's responsibilities for authoring, administering, and executing any and all test cases.
  - A.10.10.8.10 The key stakeholders and their roles for each of the testing phase, including but not limited to the Contractor resources, State's business and technical resources, and other State Contractors.
  - A.10.10.8.11 The strategy for retesting failed test cases to ensure early identification and remediation of potentially persistent project issues.
  - A.10.10.8.12 The strategy for communicating testing progress, status, and outcomes across each testing phase by module, highlighting variances in module characteristics that require modification to accurately communicate testing progress.
  - A.10.10.8.13 The strategy/process for determining test success criteria and reaching agreement with State on passing results for various test types.
  - A.10.10.8.14 The entry and exit criteria for each testing phase, including the appropriate Gate Reviews and success factors for each phase.
  - A.10.10.8.15 The testing documentation that shall be produced to support IV&V activities.
- A.10.10.9 The Contractor Shall ensure that the Test Management Plan, at a minimum, incorporates the following as needed and agreed upon by the State:

- A.10.10.9.1 Unit Testing
- A.10.10.9.2 Smoke/Sanity Testing
- A.10.10.9.3 Functional Testing
- A.10.10.9.4 Regression Testing
- A.10.10.9.5 Ad-hoc Testing
- A.10.10.9.6 Exploratory Testing
- A.10.10.9.7 Usability Testing
- A.10.10.9.8 GUI Software Testing
- A.10.10.9.9 GUI Navigation Testing
- A.10.10.9.10 Accessibility Testing
- A.10.10.9.11 Security Compliance Testing
- A.10.10.9.12 Compatibility Testing
- A.10.10.9.13 Boundary Testing
- A.10.10.9.14 Negative Testing
- A.10.10.9.15 Error Handling Testing
- A.10.10.9.16 Alert/Monitoring Testing
- A.10.10.9.17 Capacity Testing
- A.10.10.9.18 Performance Testing
- A.10.10.9.19 Recovery Testing
- A.10.10.9.20 Reliability Testing
- A.10.10.9.21 End-to-End Testing – End-to-End Testing shall include scenarios-based test cases that cover the lifecycle of an application, from entry into the Solution, through Eligibility Determination noticing and appeals.
- A.10.10.9.22 Enterprise Testing
- A.10.10.9.23 User Acceptance Testing – The State shall have access to Contractor test cases during User acceptance testing.
- A.10.10.9.24 Operational Readiness Testing – This testing shall ensure that the operational readiness testing is appropriately comprehensive and inclusive of all elements of the State enterprise impacted by the TEDS Release deployment.
- A.10.10.9.25 Business Rules Testing

- A.10.10.9.26 Availability Testing
- A.10.10.9.27 Interface Testing
- A.10.10.9.28 Beta Testing
- A.10.10.9.29 Conversion Testing
- A.10.10.9.30 Component Integration Testing
- A.10.10.9.31 Quality Control Testing
- A.10.10.10 The Contractor shall review the Test Management Plan with the necessary stakeholders prior to beginning test activities and secure State approval of the Test Management Plan by the State designated testing lead prior to any tests being executed.
- A.10.10.11 The Contractor shall execute the Test Management Plan and deliver all test requirements.
- A.10.10.12 The Contractor shall conduct a review of the Test Management Plan with the State at the completion of each Release to assess its effectiveness and determine any necessary adjustments to the Test Management Plan, and shall make necessary approved changes to the Test Management Plan as identified through this review process.
- A.10.10.13 The Contractor shall support the State on program level testing of the information security requirements.
- A.10.10.14 The Contractor shall include appropriate static and dynamic application security testing approaches in the Test Management Plan to ensure required levels of application security.
- A.10.10.15 The Contractor shall provide the IV&V Contractor the necessary support to facilitate IV&V Attestation.
- A.10.10.16 The Contractor shall provide the IV&V Contractor the necessary support to validate and verify all testing activities throughout the System Development Lifecycle.
- A.10.10.17 The Contractor shall provide the State the necessary support to facilitate MARS-E self-attestation requirements.
- A.10.10.18 The Contractor shall coordinate with assessment teams to provide information and remediate findings for the Security Assessment Review.
  - A.10.10.18.1 The Contractor shall coordinate with the State and other contractor's designated by the State to conduct a Security Control Assessment (SCA) both during the initial implementation and annually in subsequent M&O years.
  - A.10.10.18.2 The Contractor shall plan and facilitate SCA-related activities including, but not limited to:
    - a) Provide environments and user accesses

- b) Provide documentation
- c) Provide access to contractor personnel

A.10.10.18.3 The Contractor shall take account the lead time on each of the assessment activities required by the SCA and CMS reviews in order to meet the project time objectives.

#### A.10.10.19 Authoring Tests:

A.10.10.19.1 The Contractor shall schedule Environment Readiness Review(s) (ERRs) to include necessary State designated personnel.

A.10.10.19.2 The Contractor shall document all tests and testing activities in accordance with the Test Management Plan. Minimally every functional and non-functional requirement (including load, performance, capacity, and availability requirements) must be tested by a documented test case or cases, and each test case shall be State-approved and accompanied by the following information:

- a) The associated requirements
- b) The environment in which the test is to be performed
- c) The release in which the test case is performed
- d) The test type
- e) The data and/or test harnesses to be used in executing tests
- f) Test designer, performer, reviewer, and approver roles, to support segregation of duties and assure performance of tasks by qualified personnel
- g) Expected test results
- h) The specific steps and sequences to be performed in completing the test

A.10.10.19.3 The Contractor shall ensure that test cases account for testing of all State required browsers and versions as well as accessibility considerations specified by Section 508 and WCAG 2.0 AA standards.

A.10.10.19.4 The Contractor shall update corresponding test cases impacted by code or requirement changes based on approved changes to solution requirements, as approved by the Project Steering Committee.

A.10.10.19.5 The Contractor shall review tests with appropriate stakeholders and shall secure approval from the State designated testing lead prior to executing the tests.

A.10.10.19.6 The Contractor shall provide system security documentation with appropriate State stakeholders to facilitate security testing.

#### A.10.10.20 Executing Tests:

- A.10.10.20.1 The Contractor shall assign personnel to perform tests in alignment with the roles specified in the designated test plan(s).
  - A.10.10.20.2 The Contractor shall use current industry standard testing and defect tracking tools approved by State.
  - A.10.10.20.3 The Contractor shall use State approved automated testing tools for regression testing and as needed for other high frequency testing activities.
  - A.10.10.20.4 The Contractor shall work in conjunction with State and Strategic Technology Solutions (STS) to provide necessary environments to support all testing activities as approved and defined by State.
  - A.10.10.20.5 The Contractor shall ensure that the test performers have the necessary skills and appropriate access to perform the test(s) effectively.
  - A.10.10.20.6 The Contractor shall demonstrate and ensure that an State-approved number of staff are allocated to testing activities to efficiently deliver a quality product, maintain project schedule, and support its implementation approach.
  - A.10.10.20.7 The Contractor shall perform and document the peer review process for unit tests and test plans.
  - A.10.10.20.8 The Contractor shall document the test performer, reviewer, and approver for each test.
  - A.10.10.20.9 The Contractor shall record outcomes of the tests and re-test and provide evidence to demonstrate the complete execution of all State approved tests.
  - A.10.10.20.10 The Contractor shall document test results with the associated requirements in the Requirements Traceability Matrix.
  - A.10.10.20.11 The Contractor shall record any defects or errors as outlined in the State's Defect Management Process Software Problem Resolution Standards/Procedures Process.
  - A.10.10.20.12 The Contractor shall retest any State-failed and/or Contractor-failed tests.
  - A.10.10.20.13 The Contractor shall, in cases of recurring test failures, provide access to the related code for third party review upon request from State.
  - A.10.10.20.14 The Contractor shall re-execute all modified tests resulting from changes to solution requirements as approved by the Project Steering Committee as defined in the State's Program Governance Management Plan.
  - A.10.10.20.15 The Contractor shall provide personnel as requested by the State to participate in the Implementation Readiness Review(s) (IRRs).
- A.10.10.21 Reporting Test Status and Results:

- A.10.10.21.1 The Contractor shall publish the status of current and upcoming test activities that fall within the reporting timeline specified in the Test Management Plan.
- A.10.10.21.2 The Contractor shall secure State approval for the frequency of test reporting.
- A.10.10.21.3 The Contractor shall support State by providing ad hoc reporting for requests approved by the eligibility modernization Steering Committee.
- A.10.10.21.4 The Contractor shall customize test reports based on the intended audience.
- A.10.10.21.5 The Contractor shall secure State approval in defining test reporting metrics.
- A.10.10.21.6 The Contractor shall publish test results to include, at a minimum:
  - a) Test progress
  - b) Test results (e.g. pass, fail, deferred, failure reason by category, failure resolution, test category by module, test category by function). Failure reasons include poorly written code, poorly written test scripts, environment, etc.
  - c) Test results rates
  - d) Retest results rates
  - e) Trends of test results
  - f) Evidence files
- A.10.10.21.7 The Contractor shall provide additional analysis, as requested by State, to identify patterns in failed test cases and patterns of failures within the modules.
- A.10.10.21.8 The Contractor shall provide technical documentation as well as test results for non-functional requirements to support user acceptance testing of the completed system requirements.

#### A.10.11 Interface/Integration Management

##### A.10.11.1 Plan Interface/Integration Management Approach:

- A.10.11.1.1 The Contractor shall develop and execute a TEDS Interface/Integration Management Plan that conforms to the standards outlined in the HCFA Interface/Integration Management Plan and shall include but not be limited to:
  - a) The approach to developing and managing internal and external interfaces.
  - b) Technical tools that shall be used for extract, data transformation and loading and for resolving errors.

- c) Requirements that identify any conversion and Extract, Transform, and Load (ETL) process as needed.
  - d) A description of how the Contractor's development standards shall be reconciled, to reflect use of an Enterprise Service Bus (ESB) and web services as wrappers to legacy systems. The Contractor shall produce example scenarios for integration reflecting their infrastructure components and toolset.
  - e) Tasks, deliverables and resources necessary to complete interface development, testing, and implementation.
  - f) Test Management Plan that identifies testing management and scheduling between interface partners and all State agencies.
  - g) Automated monitoring and alerting mechanisms that shall address interface errors and provide automated escalation to all relevant stakeholders.
  - h) All interfaces that need IV&V attestation including appropriate scheduling activities associated with the attestation activities. Description of how the solution development and test systems shall work with internal and external interfaces.
  - i) Descriptions of the process for managing changes to the interfaces, both in the production and non-production environments.
  - j) List of Solution interfaces, data format, frequency of updates and expected data volume.
  - k) Process for interfacing and collaborating with interface partners, including roles, responsibilities, deliverables, priority, and timelines.
  - l) Process for ensuring that the development and test environments work with the internal and external non-production interfaces.
  - m) Communication Management Plan to establish automated monitoring and alert procedures for contacting Key Personnel in the event of interface/integration interruptions.
  - n) Communication Management Plan to establish automated monitoring and alert procedures for contacting Key Personnel in the event of the failed delivery of a scheduled interface file.
- A.10.11.1.2 The Contractor shall identify risks in the development and maintenance of interfaces and devise risk mitigation strategies.
- A.10.11.1.3 The Contractor shall ensure that integrations and interfaces are in compliance with all relevant security and privacy standards.
- A.10.11.1.4 The Contractor shall ensure integrations and interfaces appropriately address compliance with Minimum Acceptable Risk Standards for Exchanges, Social Security Administration, and Federal Tax Information security requirements.

A.10.11.1.5 The Contractor shall manage connectivity and operate in terms of Solution availability.

A.10.11.2 Document Requirements and Design:

A.10.11.2.1 The Contractor shall confirm identification of all sub-systems or sub-system components, previously identified by the State and the Technical Advisory Services Contractor, that require interfacing.

A.10.11.2.2 The Contractor shall review and, as needed, identify the interface requirements that define at a minimum the scope of work, design, development, installation, integration, testing and commissioning of the sub-systems.

A.10.11.2.3 The Contractor shall work with the State to secure necessary agreements with third parties (including CMS, relevant State of Tennessee agencies, federal institutes and other interface partners) for interfaces and integrations.

A.10.11.2.4 The Contractor shall work in cooperation with the State and Interface partners to specify the information to be exchanged over the interface by documenting this in Interface Control Documents to provide precise technical definitions of interface data flows and protocols.

A.10.11.2.5 The Contractor shall develop the Interface Control Document, based on the CMS Interface Control Document template, to document and track the necessary information required to effectively define the TEDS interfaces as well as any rules for communicating with them in order to give the development team guidance on architecture of the system to be developed.

A.10.11.2.6 The Contractor shall validate all interface control documents with the State Security team.

A.10.11.2.7 The Contractor shall specify and be managed to performance and availability criteria, subject to State approval, for each interface or integration including but not limited to budget, uptime requirements, outage coverage, maintainability, scalability, sustainability, portability, efficiency and usability.

A.10.11.3 Develop Interfaces and Integrations:

A.10.11.3.1 The Contractor shall plan and develop interfaces and/or integrations to support, manage, and monitor the timely and accurate exchange of information between the TEDS and all other necessary systems, including but not limited to the Federal Data Services Hub (FDSH), State of Tennessee Department of Human Services, Strategic Technology Services (STS), Social Security Administration (SSA) and other federal and state external data sources as needed (see Contract Attachment 5).

a) The Contractor shall coordinate and collaborate with third-party vendors with regards to operational interfaces for existing systems.

b) The Contractor shall plan and develop interfaces and/or integrations for all newly developed systems.

- A.10.11.3.2 The Contractor shall manage and operate the interface connection between the TEDS and the FDSH.
- A.10.11.3.3 The Contractor shall provide for secure and real-time data exchanges during operation of the TEDS.
- A.10.11.3.4 The Contractor shall obtain approval by the State Information Security Steering Committee or its designated proxy on Interface Design Documents to ensure appropriate access to information when executing data exchanges.
- A.10.11.3.5 The Contractor shall coordinate integration efforts with Interface Partners and all State agencies.
- A.10.11.3.6 The Contractor shall provide control mechanisms for each integration, to ensure successful and complete exchange of all interface and integration data.
- A.10.11.3.7 The Contractor shall provide fail-over approaches to address high availability, prevent service interruptions, and ensure system availability due to maintenance or unanticipated events.

#### A.10.11.4 Test Interfaces and Integrations:

- A.10.11.4.1 The Contractor shall provide control mechanisms for each integration, to ensure successful, appropriate, and complete exchange of all specified data elements.
- A.10.11.4.2 The Contractor shall establish an escalation plan, approved by the State, for the resolution of issues in the event that interface partners cannot come to an agreement.
- A.10.11.4.3 As part of the Test Management Plan, the Contractor shall develop, manage, and monitor testing schedule and use it to coordinate with all Interface Partners.
- A.10.11.4.4 The Contractor shall test all relevant elements of interfaces and interchanges in conjunction with HCFA IS and provide supporting documentation of successful test completion to the State and secure State sign-off, documenting completion of the integrations and interfaces to the specified state requirements. These tests shall demonstrate accuracy, completeness, timeliness, and performance of interfaces and interchanges.
- A.10.11.4.5 The Contractor shall conduct End-to-End testing with the State's interface partners after completion of system testing, and define the Solution entry and exit criteria for this phase of testing with State approval.
- A.10.11.4.6 The Contractor shall develop the necessary test cases and scenarios to validate and verify Solution interfaces function as expected by requirements. To this end, boundary value testing, negative testing, and white and black box testing approaches shall be incorporated into the test cases and scenarios, as well as communicated to the appropriate Interface partners, to ensure proper test coverage and collaboration,

- A.10.11.4.7 The Contractor shall provide test data and test harnesses where appropriate to State IS.
- A.10.11.4.8 The Contractor shall provide the IV&V Contractor the necessary support to facilitate IV&V Attestation.

A.10.11.5 Deploy Interfaces and Integrations:

- A.10.11.5.1 The Contractor shall ensure completion/readiness of all designated interface and integration deployment risk mitigation plans.
- A.10.11.5.2 The Contractor shall participate in pre-deployment Gate Reviews and provide documentation to ensure readiness of interfaces and integrations for deployment.
- A.10.11.5.3 The Contractor shall deploy all approved interfaces and integrations into production, following an agreed upon change, configuration, deployment and release management procedures.
- A.10.11.5.4 The Contractor shall ensure successful deployment of the interfaces and integrations through smoke test results or other processes as agreed by the State.

A.10.11.6 Operate Interfaces and Integrations:

- A.10.11.6.1 The Contractor shall establish automated monitoring and alert procedures for contacting Key Personnel in the event of interface/integration interruptions in real time, available twenty-four (24) hours per day, seven (7) days per week, and three hundred and sixty-five (365) days per year (24/7/365).
- A.10.11.6.2 The Contractor shall track, validate, and report completion of all specified data exchange activities.
- A.10.11.6.3 The Contractor shall track, report, and analyze all interface and integration exceptions and errors and shall work with interface and integration partner entities and the State's operations as needed to identify a resolution path and communication plan for the errors.
- A.10.11.6.4 The Contractor shall manage and adhere to the State's Software Problem Resolution process for investigating and resolving reported problems and potential defects.
- A.10.11.6.5 The Contractor shall monitor the need for interface and integration changes and shall follow the technical change control process to initiate approval for changes.
- A.10.11.6.6 The Contractor shall update interfaces and integrations, as approved through the HCFA Technical Change Control Board, to address new requirements and achieve continued or improved effectiveness in meeting existing requirements.
- A.10.11.6.7 The Contractor shall ensure that there is root-cause analysis performed for all unexpected service interruptions due to failed interfaces/integrations.

- A.10.11.6.8 The Contractor shall identify and develop recovery and any needed remediation procedures for known errors
- A.10.11.6.9 The Contractor shall identify and develop approved escalation procedures.
- A.10.11.6.10 The Contractor shall coordinate with HCFA and develop a BC/DR plan in compliance with State and Federal requirements supporting the State's ATC.

#### A.10.12 Integrated System Implementation Management

##### A.10.12.1 Develop Implementation and Deployment Plan:

- A.10.12.1.1 The Contractor shall develop and execute an Implementation and Deployment Plan consistent with the standards outlined in the CMS Implementation Plan Template, to define the activities, sequence, roles and responsibilities associated with moving the TEDS into production. Production cut-over shall accommodate a multi-phased approach. This plan shall include at a minimum:
  - a) Outline the deployment approach.
  - b) Define the entry criteria required to commence deployment activities.
  - c) Provide the names of the responsible organization(s), and titles and telephone numbers of the staff who serve as points of contact for the deployment. These points of contact shall include the Contractor Project Manager and Technical Lead and Key Personnel, the State technical and business owners, the State key resources, as well as Other State Contractors and representatives from other entities such as STS, CMS, and State of Tennessee Department of Human Services.
  - d) Define the timeline and schedule of deployment activities.
  - e) Document deployment risks and provide detailed risk mitigation plans.

##### A.10.12.2 Develop Roll Back Plan

- A.10.12.2.1 Define and execute a Roll Back Plan for the State's approval, to provide a contingency option in case of deployment complications or failure, to include at a minimum:
  - a) Criteria required for a roll back to occur
  - b) Defined sequence of events prior to and during execution of a CP
  - c) Communication matrix including stakeholders to contact in the event a roll-back or CP must occur
  - d) Escalation process

- A.10.12.3 Document criteria for implementing the system in the production environment and necessary documentation required to proceed with the implementation process.
- A.10.12.4 The Contractor shall develop and execute a System Maintenance, Support, and System Transition Plan.
  - A.10.12.4.1 The Contractor shall document the entry and exit criteria for transition activities, as approved by the State, to commence and complete transition to operations.
  - A.10.12.4.2 The Contractor shall describe the Contractor's approach for supporting a multi-phased release of functionality to provide the State value as early as possible during the project timeframe.
  - A.10.12.4.3 The Contractor shall document the Contractor's approach, resources, and organizational structure to support efficient Operations and Maintenance activities including approved workarounds, enhancements and defect fixes for software CIs included in the production release while simultaneously supporting major software CIs in development for subsequent releases.
  - A.10.12.4.4 The Contractor shall document the Contractor's approach, resources, and organizational structure to support efficient development of software CIs for future functionality releases without compromising Operations and Maintenance activities for software CIs in production.
  - A.10.12.4.5 The Contractor shall describe the approach for issue reporting and resolution of issues identified during the post go-live stabilization period prior to the post implementation review.
  - A.10.12.4.6 The Contractor shall document exit criteria, including service level agreements and applicable performance standards that shall be used to define a stable production environment, as well as the required duration for stable performance to ensure completion of the stabilization period. Exit criteria shall be contingent on State approval.
  - A.10.12.4.7 The Contractor shall document assumptions, constraints, dependencies, risks and issues applicable to the transition to operations.
  - A.10.12.4.8 The Contractor shall identify risk mitigation plans and owners for transition activities.
  - A.10.12.4.9 The Contractor shall develop and execute a Cut-Over Plan as described in Section A.15.1 that provides continuity of service in Medicaid and CHIP for the State of Tennessee.
  - A.10.12.4.10 The Contractor shall develop a plan to manage the activities and issues related to the transition from a determination to an assessment state.
  - A.10.12.4.11 The Contractor shall prepare CMS required change control documentation that applies to significant changes in compliance with CMS change management process.
- A.10.12.5 Prepare for Implementation

- A.10.12.5.1 The Contractor shall provide information as requested by the IV&V Contractor to ensure that the system is fully compliant with functional and non-functional requirements, configuration management requirements, and service level agreements.
- A.10.12.5.2 The Contractor shall complete implementation preparation activities that shall be used to drive a 'Go/No-Go' decision, including at minimum:
- a) Completion of a holistic Operational Readiness Assessment that shall outline critical system and business components, and each individual/business unit required to provide sign-off
  - b) Demonstrated completion of entry criteria for the start of implementation activities, as defined in the Implementation and Deployment Plan, with sign-off from the State.
  - c) Provision of implementation checklists, for final approval by the State, to support accurate completion of all implementation activities.
- A.10.12.5.3 The Contractor shall request a 'Go/No-Go' decision from the State and shall receive a 'Go' decision prior to entering into implementation activities.
- A.10.12.5.4 The Contractor shall plan and execute an appropriate communication strategy for all implementation affected stakeholders in cooperation with the State's OCMT personnel and Strategic Program Management Office personnel.
- A.10.12.5.5 The Contractor shall support training activities in conjunction with the State and other state contractors.
- A.10.12.6 Execute Implementation and Deployment Plan:
- A.10.12.6.1 The Contractor shall follow the implementation documentation, checklists, and tools developed in the Plan Implementation activity to support successful completion of a system implementation.
- A.10.12.6.2 The Contractor shall complete implementation execution activities once a 'Go/No-Go' decision has been reached, including at minimum:
- a) Deployment activities to occur upon receiving State approval for implementation
  - b) Overall sequence and site-specific implementation specifications
  - c) Manage coordination activities with Strategic Technology Solutions (STS) and all interface partners.
  - d) Management of Operations and Maintenance resources
  - e) As needed, execute CPs as defined in the Implementation and Deployment Plan activity.
- A.10.12.6.3 The Contractor shall provide Release Notes that outline the overall implementation process.

A.10.12.6.4 The Contractor shall convert data from existing data sources associated with the specific release, and perform substantial initial data loads from legacy operational systems.

A.10.12.7 Execute Transition Plan:

A.10.12.7.1 The Contractor shall provide the appropriate level of resources and organizational structure to support efficient Operations and Maintenance activities including bug fixes and enhancements for software CIs included in production release while not compromising productivity for major software CIs in development.

A.10.12.7.2 The Contractor shall ensure that Operations and Maintenance staff is trained, onsite, ready and capable of providing Operations and Maintenance services four (4) weeks prior to go-live.

A.10.12.7.3 The Contractor shall provide State-approved quantity of personnel to the Operations and Maintenance production control that shall include at a minimum Configuration/Release Manager, Continuous Improvement Process (CIP), Problem/Incident Manager, and a Production Control/Operations Manager.

A.10.12.7.4 The Contractor shall provide the appropriate level of resources and organizational structure to support efficient development of software CIs for future functionality releases while not compromising O&M activities for software CIs in production.

A.10.12.7.5 The Contractor shall publish risk and issue reporting and resolution.

A.10.12.7.6 The Contractor shall identify and execute resolution plans, subject to State approval, for any issues identified during the post go-live warranty period prior to the post implementation review.

A.10.12.7.7 The Contractor shall ensure satisfactory completion of transition exit criteria as defined in the State's Implementation and Deployment Plan and performance levels as identified in relevant service level agreements.

A.10.12.7.8 The Contractor shall complete full fail-over testing with all system monitoring activities in place.

A.10.13 Post Implementation Evaluation

A.10.13.1 Support evaluation planning:

A.10.13.1.1 The Contractor shall provide information to indicate availability and schedule for providing data to support the evaluation.

A.10.13.1.2 The Contractor shall provide prototypes of data to confirm fit and format of data to support the post implementation evaluation.

A.10.13.2 Provide information

A.10.13.2.1 The Contractor shall provide data, as specified and in a format approved by the State, to document Solution performance, and supports user/customer and performance assessment activities.

A.10.13.2.2 Provide required deliverables as outlined in the post-implementation review Gate Review.

A.10.13.3 Provide recommendations

A.10.13.3.1 The Contractor shall document lessons learned.

A.10.13.3.2 The Contractor shall provide the State with documentation of lessons learned, as compiled through the lifecycle and in the Post-Implementation Evaluation, to support improved project performance on future Solution Releases and, where applicable, other MMP projects, to include topics such as:

- a) Best practice identification
- b) Issue root causes
- c) Risk and issue mitigation
- d) Performance improvement opportunities

A.10.13.3.3 The Contractor shall provide recommendations for process improvement to the system development lifecycle.

A.10.13.3.4 The Contractor shall participate in lessons learned activities for each release and provide constructive feedback, both positive and negative, with respect to their role in the Solution lifecycle.

A.10.13.3.5 The Contractor shall provide Solution recommendations, supported by analysis to include cost, risk, security, business, and organizational impacts, and that outline:

- a) Functions that may warrant refinement or replacement to support improved performance or architectural alignment
- b) Functions that may warrant enhancement, to derive increased value from the existing Solution investment
- c) New functions that can provide compelling value in addressing the State's business needs.

A.10.13.4 The Contractor shall engage in Annual Operational Assessments (AOAs) that reports on:

A.10.13.4.1 Performance of the Solution

A.10.13.4.2 User satisfaction with the Solution

A.10.13.4.3 Adaptability to changing business needs

A.10.13.4.4 New technologies that might improve the investment

#### A.10.13.5 Develop/Implement Enhancements

- A.10.13.5.1 Upon determination by the State that enhancements (changes and modifications to the system during O&M, over and beyond original specifications and requirements) are warranted, the Contractor shall create an Enhancement Change Order for the State's approval. Enhancement Change Orders shall follow the Change Order process defined in Section A.28 below.
- A.10.13.5.2 The Contractor and the State shall prioritize, document, implement, and test enhancements based on the HCFA Technical Change Control Process.
- A.10.13.5.3 Enhancement activities are in addition to the O&M activities and shall be performed by separate Contractor staff.
- A.10.13.5.4 The Contractor shall complete Service Design Packages describing changes to original design documents when enhancements impact technical designs.

#### A.10.13.6 Disposition Plan

- A.10.13.6.1 The Contractor shall develop and execute a Disposition Plan in compliance with the CMS System Disposition Plan.
- A.10.13.6.2 The Contractor shall include project closeout activities, data archiving strategies, hardware destruction procedures, and capacity reallocation in the Disposition Plan.
- A.10.13.6.3 The Contractor shall review the Disposition Plan and obtain State approval.

#### A.11 Deliverable Submission Process

- A.11.1 The Contractor shall follow the defined deliverable submission process for each deliverable included in the Table of Deliverables (Section A.27) below. The Contractor may submit additional steps which shall be documented in the PMP.
- A.11.2 At a minimum, the Contractor shall submit a DED via the CM process for each deliverable at least one month prior to the first submission date and request approval from the State.
- A.11.3 The Contractor shall create deliverables as defined in each approved deliverable's DED.
- A.11.4 The Contractor shall facilitate for each deliverable a minimum of one walkthrough with the State one week prior to the deliverable submission date.
- A.11.5 The Contractor shall submit for each deliverable a first submission on the agreed submission date and allow the State to review and provide responses.
- A.11.6 The Contractor shall submit for each deliverable a subsequent submission, resolving comments received by the State on the previous submission, and allowing the State to review and provide responses.

- A.11.7 The Contractor shall resolve all outstanding responses from the State prior to each deliverable's final submission.
- A.11.8 The Contractor shall submit a final (as of the particular Gate Review) submission for each deliverable at least six (6) weeks prior to a State Gate Review and/or CMS Gate Review.
- A.11.9 The Contractor shall submit a final submission for each deliverable at least three weeks prior to a Project Consult.
- A.11.10 The Contractor shall follow the review and response times based on the complexity level bucket assigned to the deliverable in the Table of Deliverables (Section A.27), as follows:

*Table 1: Table of Deliverables*

<b>Deliverable Classification</b>	<b>Length of State Review Period for each Review Cycle</b>	<b>Length of Contractor Update Period after Receiving State Updates</b>
<b>Type A</b>	Seven (7) days	Seven (7) days
<b>Type B</b>	Ten (10) days	Ten (10) days
<b>Type C</b>	Twenty (20) days	Twenty (20) days

#### A.12 System Requirements

- A.12.1 Contractor shall ensure that the Solution meets the State's functional and non-functional requirements. In building the Solution, Contractor shall comply with those requirements, contained in this Contract, including but limited to, those contained in Contract Attachment TBD [CONTRACTOR'S NEGOTIATED RESPONSE TO Contract ATTACHMENT TBD].
- A.12.2 The Contractor's Solution shall automate all of the defined functional requirements, unless otherwise stated within the respective requirement language approved by the State.

#### A.13 Environments

- A.13.1 The Contractor shall build, support, document, and maintain the environments necessary to support all releases of the TEDS. This includes, but is not limited to, development, data conversion, testing, training, operational readiness, and production. Environments shall be housed and hosted by the State's STS.
- A.13.2 The Contractor shall develop and document an environment strategy and approach that shall ensure State-approved environments to support all requirements defined within the Contract.
- A.13.3 The environment strategy and approach shall support the need for two concurrent releases in development, in addition to regular maintenance releases. Therefore, a minimum of four (4) sets of development and testing environments shall be required.
- A.13.4 The Contractor shall provide the environments below. Any deviation from the list of environments below shall be supported by the Contractor's environment strategy and approach and approved by the State. The Contractor may utilize additional application environments based on their development methodology and their understanding of the project roadmap.

##### A.13.4.1 Production Environment with Failover Clustering

- A.13.4.2 Production Support Environment with Failover Clustering
  - A.13.4.3 Staging/Penetration Testing Environment with Failover Clustering
  - A.13.4.4 Technical Sandbox Environment
  - A.13.4.5 Development Environments
    - A.13.4.5.1 Development Environment
    - A.13.4.5.2 Interface Development Environment
    - A.13.4.5.3 Unit/Automated Test Environment
    - A.13.4.5.4 Component Integration Test Environment
    - A.13.4.5.5 Conversion Development Environment
  - A.13.4.6 Test Environments
    - A.13.4.6.1 System Integration Test Environment
    - A.13.4.6.2 Functional Test Environment
    - A.13.4.6.3 Automated Regression Test Environment
    - A.13.4.6.4 Interface Test Environment
    - A.13.4.6.5 Performance/Stress Test Environment with Failover Clustering
    - A.13.4.6.6 Conversion Test Environment
    - A.13.4.6.7 User Acceptance Test Environment
    - A.13.4.6.8 Quality Control Testing Environment
    - A.13.4.6.9 Beta Test Environment
  - A.13.4.7 Training Environment
  - A.13.4.8 Disaster Recovery Environment with Failover Clustering
- A.14 Data Conversion
- A.14.1 The Contractor shall be responsible for planning, developing, testing, implementing, maintaining, and managing the secure data conversion process in all environments of the TEDS.
  - A.14.2 The Contractor shall identify the legacy systems and other data sources, as determined by the State, to be loaded into the Solution.
  - A.14.3 The Contractor shall be responsible for converting all data from all legacy eligibility determination systems that are necessary for the TEDS to support ongoing eligibility determinations, redeterminations, appeals, audits, and other processes as required by Federal and State regulations and policies.

- A.14.4 The Contractor shall document and recommend selection criteria to the State to be used to identify the data to be extracted (by the State) from the source data.
- A.14.5 The Contractor shall define and document whether the data conversion process for a data source shall be an automated data conversion process or a manual data conversion process.
- A.14.6 The Contractor shall provide an explanation indicating the reason an automated conversion of a data source is not feasible or otherwise not recommended.
- A.14.7 The Contractor shall provide details on data collection tools and load processes for any data conversion processes that are identified as necessary.
- A.14.8 The Contractor shall provide logical and physical data models for the TEDS, including but not limited to, an Entity Relationship Diagram, Data Flow Diagram, and Data Dictionary.
- A.14.9 The Contractor shall provide a detailed data element mapping crosswalk between the data sources and the data target.
- A.14.10 The Contractor shall map source data elements to target data elements with transformation rules.
- A.14.11 The Contractor shall define data cleansing, reporting, and remediation processes and procedures for each data source, with organizational roles and responsibilities.
- A.14.12 The Contractor shall provide tools to be utilized for development and execution of the Extract, Transform, and Load (ETL) processes required to complete automated data conversion.
- A.14.13 The Contractor shall provide estimated data volumes and conversion runtimes by data source.
- A.14.14 The Contractor shall describe the QA processes to be executed and reports to be delivered to HCFA IS to verify the completeness, integrity, and readiness of the converted data for use in the Target system.
- A.14.15 The Contractor shall define reconciliation processes to track the ETL process for each row from source to target system.
- A.14.16 The Contractor shall define change control authorization and audit processes to authorize and track changes applied outside of the Solution to converted data in order to correct errors identified in the data during pre or post Go-Live of the Solution following the data conversion.
- A.14.17 The Contractor shall be responsible for the development of conversion software and performing manual data conversion. This activity shall include testing conversion programs and procedures and the preliminary conversion of all data.
- A.14.18 The Contractor shall be responsible, through facilitation with the State, for coordinating and collaborating with other necessary contractors to resolve data conversion issues.
- A.14.19 The Contractor shall be responsible for maintaining the data after go-live and ensure that maintenance of the source DBMS after Go-Live does not adversely impact the referential integrity of the data.

- A.14.20 The Contractor shall be responsible for maintaining an original copy of the source conversion data to be used during testing within a staging area in the data conversion database(s).
- A.14.21 The Contractor shall be responsible for reconciling and vetting data source (e.g., CHIP, MMIS, Accent data) mapping errors and allotting the appropriate timing to correct these errors prior to converting the data into the target system.
- A.14.22 The Contractor shall be required, at the direction of the State, to directly work with the State and other State contractors to analyze the data to be converted and develop extract specification and testing processes to ensure completeness of data conversion.
- A.14.23 The Contractor shall provide an Extract Control Document, as a part of the Data Conversion and Synchronization Plan defined in Section A.27, for each data source.
- A.14.24 The Contractor shall coordinate with the State and other State contractors to develop a Data Conversion and Synchronization Plan describing the approach, strategy, constraints, assumptions, and specifications for converting and migrating data from current legacy sources.
- A.14.25 The Contractor shall develop and deliver to State stakeholders, and execute a comprehensive Data Conversion and Synchronization Plan. The Data Conversion and Synchronization Plan shall be reviewed and baselined for each Release of the TEDS. The Data Conversion and Synchronization Plan shall include, but is not limited to, the following:
  - A.14.25.1 Identification of source and target systems/environments
  - A.14.25.2 Provision for a non-disruptive conversion (no or minimal down-time)
  - A.14.25.3 Description of any automated methods of conversion that require limited intervention by the State
  - A.14.25.4 Description and addressing of security measures that shall enforce referential integrity of all data
  - A.14.25.5 A mechanism for identifying and reporting conversion errors
  - A.14.25.6 A mechanism for error resolution
  - A.14.25.7 A method to reconcile data and differentiate between converted data and new system data
  - A.14.25.8 Provision of a capability to automatically reverse or undo a conversion
  - A.14.25.9 Identification of conversion validation and verification procedures and activities required for system testing.
  - A.14.25.10 Identification of the testing tools and scripts and the validation and verification of resulting test data, in preparation for data loading.
  - A.14.25.11 Provision of a mapping of the source to destination, considering intermediate processing requirements.

- A.14.25.12 Data cleansing process, including but not limited to, usage of HCFA's 4-match or 7-match processes
- A.14.25.13 Frequency of data conversion in all environments (such as Component Integration Testing /SIT, UAT, and Production)
- A.14.25.14 Sequencing of data loads
- A.14.25.15 Data Conversion Schedule
- A.14.25.16 Roles and Responsibilities
- A.14.25.17 Confirmation/denial of the need for parallel runs of the old and new systems during the conversion process or a one-time cut-over to the new system.
- A.14.25.18 Identification of criteria for a Go/No-Go decision.
- A.14.25.19 Assumptions
- A.14.25.20 Risks, including workarounds in the event that data conversion will be significantly delayed.
- A.14.25.21 List of tools needed to execute the conversion
- A.14.25.22 Strategy for data QA and control
- A.14.25.23 Strategy for populating data not contained in legacy systems/sources
- A.14.25.24 Approach for converting and migrating scanned documents/images from legacy systems
- A.14.26 The Contractor shall define and document how referential integrity of all the data will be maintained, both during and after the conversion process.
- A.14.27 The Contractor shall develop manual conversion procedures for loading data that cannot load to the Target new system environment using an automated conversion process. The Contractor shall be responsible for all activities required for Target system for manual data conversion.
- A.14.28 The Contractor shall produce a before-and-after conversion report to the State which shall include, but is not limited to, the following:
  - A.14.28.1 Conversion count
  - A.14.28.2 Conversion errors
  - A.14.28.3 Error rate
  - A.14.28.4 Data type conversion source type to native type failures
  - A.14.28.5 Validation and completeness for conversion
- A.14.29 The Contractor shall reconcile any errors produced from any data conversion run.

- A.14.30 The Contractor shall ensure that as a result of the data conversion process any eligible member maintains his/her Medicaid and CHIP healthcare coverage before and after the production data conversion.
- A.14.31 The Contractor shall ensure that converted data follows the protection and privacy protocols established by the SSP and security control outlined by the State and security compliance regulations. Security measures shall be enforced regarding data sensitivity issues.
- A.14.32 The Contractor shall identify the data cleansing, validation, and initiation requirements for the data conversion activities.
- A.14.33 The Contractor shall provide to the State a list of data conversion tools and the scripts used to perform data conversion, intermediate data processing, and loading cleansed data into the destination or target data repository. This shall include both automated conversion program and manual data entry procedures.
- A.14.34 The Contractor shall provide a Contingency Plan for all data conversion runs.
- A.14.35 The Contractor shall be responsible for coordinating, addressing, and reconciling with the State any data QA and control issues prior to a given data conversion cycle. In addition, the Contractor shall be responsible for identifying types of data quality problems that may occur, including but not limited to the following considerations:
- A.14.35.1 Invalid Content
  - A.14.35.2 Data Type redefinitions (e.g., alphas in dates, numbers in data field [including but not limited to Zip Codes and SSNs that have leading zeroes]).
  - A.14.35.3 Incomplete records (e.g., uninitialized data)
- A.14.36 The Contractor shall be responsible for running a number, as approved by the State, of mock data conversions to achieve a one hundred percent (100%) pass rate. Each mock conversion shall simulate the real go-live process with live data and actual volumes.
- A.14.36.1 The pass rate shall be determined by the accumulative average of all records correctly converted in every field, in every extract file, coming from the data sources. For a record to be correctly converted, the target record must either:
    - a) Match exactly how it is in the data source
    - b) Match in accordance with the detailed data element mapping crosswalk.
- A.14.37 The Contractor shall not use default values in production for missing data (e.g., SSN, birth date) without written prior approval by the State.
- A.14.38 The Contractor shall define a process to ensure that any changes to data model design due to change requests or additional functional requirements are promptly addressed in the conversion efforts and do not negatively impact the Go-Live time table or schedule.
- A.15 Operational Readiness
- A.15.1 Cut-Over

- A.15.1.1 The contractor shall create a Cut-Over Plan that describes the Contractor's approach to the following Cut-Over activities:
  - a) Coordination of all cutover activity to include verification of final data transfers, initiation of all batch jobs, cutover of network and telecommunication services, and any and all other activity defined in the Contractors approach
  - b) License and warranties for any and all hardware and software
- A.15.1.2 Cutover of the Service Desk service
- A.15.1.3 Validation of cutover success or execution of any required contingency activity in response to cutover failures
- A.15.2 The Contractor shall develop a State-approved Operational Readiness Checklist to determine whether the system is ready for go live. This checklist shall include, but not be limited to:
  - A.15.2.1 In conjunction with the State, the Contractor shall complete any remedial actions, all operator and user training for the support staff, and all privacy, security and accreditation activities.
  - A.15.2.2 The Contractor shall ensure that all components of the system function correctly and interface properly with other components.
  - A.15.2.3 The Contractor shall ensure that data conversion efforts have been assessed through System Integration Testing and User Acceptance Testing for completeness and accuracy.
  - A.15.2.4 The Contractor shall ensure that all interfaces including FDSH, state data sources and MMIS are connected to production sites, tested and verified against production, refreshed, and working per approved Functional Design Documentation and Technical Design Documentation.
    - A.15.2.4.1 The Contractor shall leverage existing MMIS interface definitions and transaction file specifications as documented in the MMIS Interface Specifications.
  - A.15.2.5 The Contractor shall ensure that the Solution can accept, store, associate and process data received through applications and interfaces.
  - A.15.2.6 The Contractor shall ensure that the Solution can log Solution errors and alerts, stakeholders are notified and appropriate resolution steps are taken within a timeframe approved by the State.
  - A.15.2.7 The Contractor shall ensure that the Solution can make correct eligibility determinations according to approved Functional Design Documentation and Technical Design Documentation.
  - A.15.2.8 The Contractor shall ensure that the Solution can generate correct and complete notices according to approved Functional Design Documentation and Technical Design Documentation.

- A.15.2.9 The Contractor shall validate Backup and Recovery operations, and provide Backup and Recovery results to the State for review and approval.
- A.15.2.10 The Contractor shall resolve all critical and high-priority defects prior to Go Live.
- A.15.2.11 The Contractor shall develop and update the Operations & Maintenance Manual and job aids that describe how to use and maintain the Solution from a business function perspective.
- A.15.2.12 The Contractor shall identify key production cut-over risks and develop mitigation plans.
- A.15.2.13 The Contractor shall ensure that role-based access, security and privacy standards are in place as part of the Solution testing and implementation.
- A.15.2.14 The Contractor shall demonstrate the Solution's ability to accurately perform hourly, daily, weekly, monthly, quarterly, and annual operational cycles.
- A.15.2.15 The Contractor shall validate that the deployed Solution is in alignment with the approved configuration baseline, included within the System Operations Documentation defined in Section A.27, and in conformance with the State's Enterprise Architecture standards.
- A.15.2.16 The Contractor shall identify variances between the deployed Solution and approved configuration baseline and take corrective actions, as approved by the State.
- A.15.2.17 The Contractor shall identify resources for Help Desk Support, Service Desk Support and Implementation Support.
- A.15.2.18 In conjunction with the State, the Contractor shall ensure that the Support resources are staffed (in terms of both numbers and skill sets) to implement and execute operational readiness activities.
- A.15.2.19 The Contractor shall define the Help Desk structure and ensure Operational procedures are documented, approved by the State, and in place.
- A.15.2.20 The Contractor shall provide an emergency on-call list for critical level defects and procedures for notifying the State in the event of a critical production defect.
- A.15.2.21 The Contractor shall designate project technology resources to perform technical support tasks.
- A.15.2.22 The Contractor shall ensure that the User Satisfaction Measurement processes are in place.
  - A.15.2.22.1 The Contractor shall ensure that metrics to assess system impact of program and performance goals are in place.
- a) The Contractor shall provide a Metrics Report to the State for review and approval.
- A.15.3 The Contractor shall be responsible for managing a process to identify, analyze, and resolve issues generated from operational readiness activities.

A.15.4 The Contractor shall conduct, at a minimum, two (2) walkthroughs of the Operational Readiness Plan.

A.15.4.1 The first walkthrough shall occur prior to the Beta Test.

A.15.4.2 The second walkthrough shall occur after the completion of the Beta Test.

A.15.5 The Contractor shall start operational readiness activities only after the State has formally communicated completion in writing of User Acceptance Testing (UAT), unless otherwise directed by the State.

#### A.16 Beta Test

A.16.1 The Contractor shall conduct a Beta Test during each implementation release.

A.16.2 The Contractor shall provide a dedicated Beta Test environment for the State to complete Beta Test activities. Beta Test shall run for a minimum of four (4) consecutive weeks, unless increased by the State, after successful exit of UAT and initial walkthrough of the Operational Readiness Checklist.

A.16.2.1 The Beta Test shall run concurrently with standard business operations and shall involve real-time processing of live application data.

A.16.3 During Beta Test, the Contractor shall confirm via reports that all daily, weekly, monthly, quarterly, and annual batch jobs and processes are operating as defined in the Functional Design Documentation and Technical Design Documentation.

A.16.4 During Beta Test, the Contractor shall confirm that all Interfaces are operating as defined in the Functional Design Documentation, Technical Design Documentation, and Interface Control Documentations.

A.16.5 During Beta Test, the Contractor shall confirm that Solution functionality, including but not limited to alert monitoring, incident management, non-functional operational readiness, and batch scheduling, are operating as defined in the Functional Design Documentation and Technical Design Documentation

A.16.6 The Contractor shall have the ability to utilize time-travel functionality during Beta Test.

A.16.7 The Contractor shall track and classify all Beta Test defects as critical, high, medium and low (as defined in the Table in Contract Attachment 2 – Liquidated Damages).

A.16.8 The Contractor shall resolve all critical and high defects prior to Go Live or, if necessary, provide the State with a written work around, downstream impacts, and plan for resolution for State review and approval.

A.16.9 The Contractor shall compare Beta Test eligibility results with legacy production eligibility results to assist in the identification of defects.

A.16.10. At the conclusion of Beta Test, the Contractor shall complete an analysis of the Beta Test and produce a Beta Test Results Report inclusive of beta test participant input, eligibility results, business process results, defects identified, defects resolved and lessons learned.

A.16.11. The Contractor shall implement a code-freeze, preventing additional updates to the software code related to the current release, upon completion of User Acceptance Testing and prior to the Beta Test period, or as required by the State.

#### A.17 Operations and Maintenance

A.17.1 The Contractor shall build and maintain a Standard Operating Procedure (SOP) Manual which shall be made available for State Staff. The manual shall be indexed, with separate sections for each capability listed with Section A.17 or otherwise identified in this Contract or specified by the State, in writing, to the Contractor. The State may require an SOP to be written for specific system support functions. The Contractor shall provide any and all tools necessary to fulfil the obligations related to executing these capabilities.

A.17.1.1 The Contractor shall execute all processes described in the SOP Manual.

A.17.1.2 The Contractor shall, at a minimum, provide the reports listed in Contract Attachment 6.

#### A.17.2 Continuous Improvement Process

A.17.2.1 The Contractor shall be responsible for managing a mature CIP for all TEDS related services throughout the entire service lifecycle.

A.17.2.2 The CIP shall identify and address opportunities for improvement within each service to maximize the service performance, value, and functionality.

A.17.2.3 The Contractor shall be responsible for developing and implementing a CIP that aligns with industry standards (e.g., ITIL or Six Sigma) and is approved by State stakeholders.

A.17.2.4 The CIP shall be reviewed and managed at the senior level within the Contractor account team to ensure effectiveness.

#### A.17.2.5 Define areas for improvement

A.17.2.5.1 The Contractor shall perform formal maturity assessments and service reviews against each capability. Assessments shall be conducted at least once a quarter, in order to highlight areas of improvement or concern. The findings of the maturity assessments and the service reviews shall be published to the State. The effectiveness of the CIP shall be demonstrated through these assessments over time, and shall be presented to the State in an annual review.

A.17.2.5.2 The Contractor shall be pro-active in its approach, developing quarterly and annual improvement roadmaps detailing initiatives on a three year cycle and set target maturity levels to measure success of the CIP.

A.17.2.5.3 The Contractor shall provide specific key performance indicators (KPIs) to be included in the analysis and require pro-active activities as the data demonstrates the need, as requested by the State.

#### A.17.2.6 Gather and process the data

A.17.2.6.1 The Contractor shall be responsible for gathering and rationalizing the supporting data for each defined KPI, and making it consistent to identify any potential gaps in the data.

A.17.2.6.2 The Contractor shall develop reports and dashboards to support the CIP and make them available to the State on a monthly basis. Reports and dashboards and the underlying KPIs shall be continuously reviewed and modified in order to mature the CIP and produce the best results.

#### A.17.2.7 Analyze the Data

A.17.2.7.1 The Contractor shall perform data analysis for all relevant services as defined within the CIP. Data analysis shall be performed at least once per quarter.

A.17.2.7.2 The Contractor shall produce a data analysis report and shall publish the report to the various State stakeholders. The data analysis report shall present an accurate picture of the results of each service performance against the defined KPIs (referenced at each capability section), allowing the State's stakeholders to have in-depth knowledge of and access to this data analysis to enhance effective managerial decision making.

#### A.17.2.8 Implement Corrective Action Plans

A.17.2.8.1 The Contractor shall provide a Solution free of defects that meets the requirements defined in this Contract. Upon identification of a defect, the Contractor shall correct any and all system or performance defects.

A.17.2.8.2 At the State's discretion, upon determination that the Solution is not correctly performing the functions required under this Contract and any applicable CM or Change Orders, the State may, through a CM and Control Directive, issue a notice to the Contractor of its intention to impose a CAP, accompanied by a request that the Contractor develop and propose an appropriate CAP for review and approval by the State within the time period designated below. The State shall determine the severity of the error using the critical, high, and medium incident definitions as set forth in the Severity Table shown Contract Attachment 2 – Liquidated Damages.

A.17.2.8.3 The State may, in its sole discretion, assess Liquidated Damages as set forth in the Liquidated Damages table located in Contract Attachment 2 – Liquidated Damages, including the enhanced CAP Liquidated Damages for more than three (3) subsequent occurrences of substantially the same issue. Each CAP shall, at a minimum, contain the following information:

- a) written documentation that includes acknowledgement of receipt of the State notice,
- b) number of impacted members and cases and such other information as the State may request
- c) a description of how the Contractor has addressed or will address the immediate problem,

- d) an analysis of the root cause of the problem, and
- e) a description of how the Contractor shall resolve the problem (or has resolved the problem) and shall prevent the problem from recurring.

- A.17.2.8.4 Upon acceptance of the CAP by the State, the Contractor shall be responsible for executing the CAP, and the CAP shall be incorporated by reference as part of this Contract. The State may request changes and/or additions to an approved CAP as deemed necessary to correct or resolve the problems that led to requesting a CAP. The Contractor shall continue to comply with an approved CAP until the State notifies the Contractor, in writing, that all problems outlined in the CAP have been satisfactorily resolved.
- A.17.2.8.5 Continued or repeated failure to prevent or forestall the same root cause error may result, in the State's sole discretion, in enhanced Liquidated Damages for Incident Resolution as set forth in Contract Attachment 2 – Liquidated Damages. In addition, such failure by the Contractor may be considered by the State to be a breach of the Contract.
- A.17.2.8.6 The Contractor shall be responsible for ensuring that all of its subcontractors or service providers comply with all approved CAPs.
- A.17.2.8.7 Notwithstanding the existence of a CAP or the CAP process, nothing in this Section relieves the Contractor of any obligations for incident resolution and/or emergency escalation processes.

### A.17.3 Service Level Management

- A.17.3.1 The Contractor is responsible and accountable for ongoing monitoring and reporting on performance against any service levels requested by and agreed upon with State leadership. At a frequency established by the State, the Contractor shall perform service level reviews. Following the Contractor's service level review, the Contractor may recommend modifications to the State. Service level agreements may be modified solely at the State's discretion.
- A.17.3.2 Monitor and Report on Service Levels
- A.17.3.2.1 The Contractor shall produce and manage a formal process for ongoing review and revision of the service levels between the State, Contractor and other State Contractors. The process shall be submitted to the State for approval within thirty (30) calendar days of contract start.
- A.17.3.2.2 The Contractor shall monitor performance against SLAs approved by the State. Reporting and monitoring of SLAs must be accurate and provide data that provides the State a complete view of the performance for each service. Reports must be provided to the State on an agreed upon regular schedule.
- A.17.3.3 Perform Service Level Reviews:
- A.17.3.3.1 The Contractor shall perform periodic reviews, on a schedule defined by the State, of SLAs and performance against them to ensure the State is satisfied with the level of performance. The Contractor shall produce and provide the State with formal reports of findings.

#### A.17.4 Service Portfolio and Service Catalog Management

- A.17.4.1 The Contractor shall work with State stakeholders to provide the necessary inputs for TEDS related services into the State's Service Portfolio and Service Catalog.
- A.17.4.2 The Contractor shall provide the relevant input to the State and other State Contractor service providers on an as-needed basis.

#### A.17.5 Technology Capacity and Performance Management

- A.17.5.1 The Contractor shall be responsible and accountable for all activities required for identifying and managing appropriate system capacity for all TEDS related systems which include production and non-production environments (e.g., Development, Test, Training, etc.). This includes requirements identification, planning, management, reporting, and augmentation of system capacity and performance.
- A.17.5.2 The Contractor shall be responsible for identifying performance and capacity drivers, understanding the impact to the program, and developing solutions to accommodate potential capacity and performance demands.
- A.17.5.3 The Contractor shall follow the agreed upon schedule for developing models, utilizing tools, and developing solutions that avoid any disruption or degradation of service. These actions shall include development of a complete set of metrics (in alignment with the program's CIP) to measure and manage system drivers including business drivers (e.g., Population, Number of Applicants, regulatory changes, etc.), the infrastructure (e.g., central processing unit, memory, bandwidth, transfer rates, storage, etc.), and other system/code related challenges (e.g., SQL code, database configurations, optimal system tuning opportunities, etc.) The Contractor shall work with the State and Service Provider (STS) to ensure the appropriate system capacity and performance is delivered.
- A.17.5.4 Monitor, Analyze, Tune and Implement
  - A.17.5.4.1 The Contractor shall draft requirements for planning, managing, and reporting system capacity in coordination with State business and IS leadership.
  - A.17.5.4.2 The Contractor shall develop a system Capacity Plan which details the requirements for planning, managing, and reporting system capacity.
  - A.17.5.4.3 The Contractor shall determine the performance drivers for performance management and their impacts on systems developed.
  - A.17.5.4.4 The Contractor shall obtain State approval relative to minimum levels of capacity the system must provide, based on consumer demand.
  - A.17.5.4.5 The Contractor shall meet the State's requirements for a maximum response time, maximum processing time for each request, and minimum number of requests that can be processed in a given period of time.
  - A.17.5.4.6 The Contractor shall draft capacity expectations for each system component.

- A.17.5.4.7 The Contractor shall monitor application and infrastructure performance 24/7/365 and perform ongoing load balancing and proactive management of systems to ensure sufficient capacity and application availability.
- A.17.5.4.8 The Contractor shall leverage industry standard tools for the monitoring, analysis and tuning of capacity and performance, which may include new or emerging technologies. Tools and technologies shall be properly vetted and approved by the State. The Contractor shall provide direct State employee access to this tool.

#### A.17.5.5 Manage Capacity and Demand

- A.17.5.5.1 The Contractor shall forecast future capacity needs based on industry standard practices to project future demand while enhancing technologies to meet demand.
- A.17.5.5.2 The Contractor shall ensure technologies are configured per State-approval to meet the forecasted peak demands and establish thresholds which shall trigger appropriate corrective action.
- A.17.5.5.3 The Contractor shall map applications and infrastructure to business processes and related demand, to measure capacity requests and consumption.
- A.17.5.5.4 The Contractor shall include cost benefit analysis as a component of the solution recommendation to the State.
- A.17.5.5.5 The Contractor shall record and track utilization of system resources to determine where capacity adjustments need to be made to support business processes as defined by the State. This shall be continually evaluated to ensure any system or environmental changes have not impacted capacity and performance.
- A.17.5.5.6 The Contractor shall estimate the required number of resources needed to support change in existing service levels and newly identified services in coordination with State business and IS leadership.
- A.17.5.5.7 The Contractor shall develop a System Capacity Plan that documents the current levels of resource utilization and service performance, and forecasts the future requirements for new TEDS infrastructure.

#### A.17.5.6 Model and Trend

- A.17.5.6.1 The Contractor shall develop demand estimates for the TEDS in coordination with State Business and IS leadership and adjust/report on estimates in accordance with the CIP reporting schedule.
- A.17.5.6.2 The Contractor shall develop a model for capacity demand based on available State data in coordination with State business and IS leadership.
- A.17.5.6.3 The Contractor shall test capacity demand prototype models to ensure they surpass demand estimates.

- A.17.5.6.4 The Contractor shall continuously update reusable sizing and estimating models to aid in capacity forecasting that utilize performance characteristics of applications based on historical data, projected load, locations, and other factors the Contractor deems appropriate.

#### A.17.5.7 Plan and Optimize

- A.17.5.7.1 The Contractor shall consult with the State on the service strategy plans for the TEDS.
- A.17.5.7.2 The Contractor shall forecast future requirements for new resources in coordination with State IS leadership to support IT services that underpin the business activities.
- A.17.5.7.3 The Contractor shall provide recommendations on resources required, costs, benefits, impacts, and other areas the Contractor or the State deem appropriate.

#### A.17.6 Availability Management

- A.17.6.1 The Contractor shall be responsible and accountable for ensuring TEDS availability and reliability is compliant with an agreed upon set of requirements for vital business functions. Responsibilities include availability planning and design in accordance with STS, risk assessment and remediation, testing, monitoring, and reporting on availability performance.
- A.17.6.2 All TEDS production systems and interfaces shall be designed for high availability (e.g. complete component redundancy, clustered solutions, data replication, and failover capabilities).
- A.17.6.3 Plan and Design for Availability
  - A.17.6.3.1 The Contractor shall draft detailed requirements for system availability in coordination with State business and IS leadership.
  - A.17.6.3.2 The Contractor shall develop a Performance and Availability Management Plan that outlines performance and availability creation and management processes and, at a minimum, meets the requirements outlined in Contract Attachment 2.
  - A.17.6.3.3 The Contractor shall meet the State's minimum target levels for availability, reliability, and maintainability of IT infrastructure components.
- A.17.6.4 Perform Risk Assessment
  - A.17.6.4.1 The Contractor shall perform regular availability risk assessments to identify and quantify risks and countermeasures to protect the availability of IT systems.
- A.17.6.5 Implement Countermeasures
  - A.17.6.5.1 The Contractor shall develop appropriate controls and countermeasures to improve the availability and resilience of TEDS services and underlying IT components.

- A.17.6.6 Test Availability & Resilience Mechanisms
  - A.17.6.6.1 The Contractor shall perform periodic, as defined by the State, availability mechanism tests to ensure that availability and resiliency mechanisms designed to provision services are operating effectively.
  - A.17.6.6.2 The Contractor shall publish an Availability and Resilience test results report and ensure they are available to State Business and IS leadership.
- A.17.6.7 Monitor, Measure, Analyze, & Report Availability
  - A.17.6.7.1 The Contractor shall leverage existing State and STS monitoring tools where available.
  - A.17.6.7.2 The Contractor shall develop availability reports to document and maintain all availability and performance analysis results conducted on the system.
  - A.17.6.7.3 The Contractor shall provide availability reports, and access to the underlying data utilized to create the reports, to the State for review during periodic service level review meetings.
  - A.17.6.7.4 The Contractor shall conduct ongoing availability and performance analysis on the system which includes monitoring the availability 24/7/365.
- A.17.7 Business Continuity/Disaster Recovery
  - A.17.7.1 The Contractor shall be responsible and accountable for ensuring the continuity of services related to the TEDS in order to ensure the business can operate effectively in the event of a disaster. The Contractor is expected to follow a rigorous, process-oriented approach which includes: business impact analysis, development of service continuity plans, risk assessments, testing, reporting, and execution of service continuity plans in the event of a disaster.
    - A.17.7.1.1 The Contractor shall participate in any enterprise BC/DR testing initiated by the State or STS.
    - A.17.7.1.2 The Contractor shall develop a Cost Benefit Analysis Plan that includes total cost of ownership, cost-benefit analysis, and weigh those costs against the desired recovery point objective/recovery time objective, providing the Cost Benefit Analysis Plan to the State for approval.
    - A.17.7.1.3 The Contractor shall incorporate training and awareness for State personnel to support BC/DR efforts as part of its BC/DR Plan.
    - A.17.7.1.4 The Contractor shall support the relationship with STS in BC/DR endeavors ensuring efforts are in line with STS. STS provides recovery support for the infrastructure. The Contractor is responsible for application recovery.
  - A.17.7.2 Initiate BC/DR

- A.17.7.2.1 The Contractor shall draft requirements for IT Service Continuity in coordination with State Business and IS leadership.
- A.17.7.2.2 The Contractor shall develop a BC/DR Plan consistent with HCFA BC/DR Management Plan and CMS Contingency Planning Guidance.
- A.17.7.2.3 The Contractor shall develop BC/DR policies and procedures in coordination with State leadership.
- A.17.7.2.4 The Contractor shall draft BC/DR guidelines in compliances with State policies and expectations.
- A.17.7.2.5 The Contractor shall draft a Backup Implementation Plan that involves virtual machines and volume snapshots.
- A.17.7.2.6 The Contractor shall develop a multiple backup approach strategy; backups being performed using backup software and backups from storage systems using snapshot technologies.
- A.17.7.2.7 The Contractor shall develop, maintain, and implement complete Versioning control processes and procedures. The Contractor shall provide any/all tools necessary to fulfil the obligations of this contract.

#### A.17.7.3 Define BC/DR Requirements & Strategy

- A.17.7.3.1 The Contractor shall perform a Business Impact Analysis (BIA) to quantify the impact of a loss of service to the State.
- A.17.7.3.2 The Contractor shall perform Risk Assessments, aligned with CMS standards, to determine areas that can be mitigated by IT and to define levels of acceptable risks to the State.
- A.17.7.3.3 The Contractor shall develop BC/DR strategies in coordination with the State leadership to achieve optimum balance of risk reduction and BC/DR options based on the results of BIAs and Risk Assessments.
- A.17.7.3.4 The Contractor shall maintain an inventory of critical system applications and processes.
- A.17.7.3.5 The Contractor shall provide a plan to comply with CMS MARS-E Contingency Plan that includes but is not limited to hoteling of Key Personnel.

#### A.17.7.4 Implement BC/DR

- A.17.7.4.1 The Contractor shall ensure that all required services, facilities, and resources are delivered in an acceptable operational state and are 'fit for purpose' when accepted by the business.
- A.17.7.4.2 The Contractor shall perform service continuity procedures as defined in the BC/DR Plan in the event of a disaster.
- A.17.7.4.3 The Contractor shall participate in enterprise BC/DR testing initiated by the State and/ or STS.

- A.17.7.5 Perform BC/DR Ongoing Operations
  - A.17.7.5.1 The Contractor shall ensure that all Contractor staff are aware of the implication of business continuity and of service continuity and consider these as part of their normal working activities.
  - A.17.7.5.2 The Contractor shall train all State and other State Contractor personnel involved in BC/DR procedures.
  - A.17.7.5.3 The Contractor shall develop and establish a program of regular DR testing, at a minimum twice a year, to ensure critical components of the BC/DR strategy can be recovered within the desired Recovery Time Objective
  - A.17.7.5.4 The Contractor shall ensure that all changes are assessed for potential impact on BC/DR plans.
  - A.17.7.5.5 The Contractor shall develop Contractor Service Continuity and Disaster reports to document and maintain BC/DR test results on a quarterly basis.
  - A.17.7.5.6 The Contractor shall provide Contractor Service Continuity and Disaster reports to the State for review during periodic service level review meetings.
  - A.17.7.5.7 The Contractor shall develop a backup job and server audit.
  - A.17.7.5.8 The Contractor shall develop and implement a testing program to include twice-yearly table-top tests, quarterly selected critical component testing, and yearly technical cut over tests.
  - A.17.7.5.9 The Contractor's BC/DR Plan shall include provisions for letter and notice processing.
- A.17.7.6 Invoke BC/DR
  - A.17.7.6.1 The Contractor shall perform all BC/DR activities when required by the State.
- A.17.8 Service Transition Planning and Support
  - A.17.8.1 The Contractor shall be responsible and accountable to develop the System Maintenance, Support and System Transition Plan and oversee the ongoing execution of the following service transition processes: Change management, configuration management, release management, and patch management. The Contractor's System Maintenance, Support and System Transition Plan and execution strategy shall follow the standards set by the State and leverage existing processes and tools as appropriate. All changes shall be approved by the State through the transition process.
  - A.17.8.2 The Contractor shall create a formalized service description and associated details when responding to business needs or proactively proposing new services.
  - A.17.8.3 The Contractor shall, during the service transition lifecycle, maintain consistent and effective communications with all impacted stakeholders.

- A.17.8.4 The Contractor shall provide a clearly defined promote-to-production process that enforces a strictly defined methodology for movement from development to quality assurance (QA) and production.
  - A.17.8.5 The Contractor shall provide full support and execute and service transitions into production or other environments.
- A.17.9 Technology Change Management
- A.17.9.1 The Contractor shall be responsible and accountable for coordinating all Technology Change Management activities to ensure that IT changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.
  - A.17.9.2 The Contractor shall define their Technology Change Management processes and procedures to ensure that all changes, including emergency, are escalated appropriately and addressed in a timely manner.
  - A.17.9.3 The Contractor shall provide industry standard automated tool for workflow tracking and approval.
  - A.17.9.4 The Contractor's Technology Change Management process shall integrate with the State Change Management process.
  - A.17.9.5 The Contractor shall work with the State change management staff to support change events identified as projects, as well as those identified as tasks (e.g. non projects).
  - A.17.9.6 The Contractor shall leverage a tool to enable the change management process, and utilize State tools where available and possible.
  - A.17.9.7 The Contractor shall provide select EMP personnel read access to change management tools and shall permit the ability to link changes to incidents/problems and vice versa. Ultimately, the State shall be responsible for approving all changes prior to promotion into the UAT and production environments.
  - A.17.9.8 Initiate Technology Change Request
    - A.17.9.8.1 The Contractor shall produce and enforce formal procedures to initiate and log requests for change (RFCs). RFCs shall provide data to allow the state to assess the change, including reason/cause, impacts, cost, schedule, and priority.
    - A.17.9.8.2 The Contractor shall provide and manage an automated Change Control Tool where changes shall be logged and managed.
    - A.17.9.8.3 The Contractor shall complete a Security Impact Analysis form and a narrative of all risks identified by the Change Request submitter with each change request.
  - A.17.9.9 Review, Assess and Authorize

- A.17.9.9.1 The Contractor shall clearly categorize changes and publish the categorization to the State for approval. Change types include normal changes, standard changes, expedited changes, and emergency changes.
- A.17.9.9.2 The Contractor shall submit a documented RFC for emergency changes within twenty four (24) hours of the change being requested.
- A.17.9.9.3 The Contractor shall publish defined RFC naming and prioritization procedures, based on business priorities and impact determinations, to ensure the State clearly understands what the change is, its priority, and potential impacts.
- A.17.9.9.4 The Contractor shall produce and receive approval from the State, policies that categorize an emergency change. These changes require the appropriate executive level approvals prior to the change being implemented.
- A.17.9.9.5 The Contractor shall produce and abide by the results of an automated risk calculation that shall recommend if the change shall be approved or denied. This calculation shall be based on system risk multiplied by the magnitude of the impact.
- A.17.9.9.6 The Contractor shall provide appropriate prioritization that is aligned with the business needs/requirements.

#### A.17.9.10 Plan and Schedule

- A.17.9.10.1 The Contractor shall produce a forward looking change schedule that accounts for all dependencies that can affect the timing of a change (e.g. year-end close activities, State regulatory requirements, open enrollments, etc.). This schedule shall also articulate downstream impacts to the overall project schedule and identify any risks and potential CPs and workarounds as appropriate.
- A.17.9.10.2 The Contractor shall manage the RFC schedule with defined and published lead times, based on risk and impact. All change windows shall be agreed upon by the State. RFC schedules shall follow the same SDLC process in use for the project.
- A.17.9.10.3 The Contractor shall comply with all MARS-E requirements and CMS guidance documents related to Change Control.

#### A.17.9.11 Build and Test

- A.17.9.11.1 The Contractor shall provide test certification and other development/testing documents required by the SDLC process and requested by the HCFA Technical Change Control Board.
- A.17.9.11.2 The testing procedures for each change shall follow the process and standards established within the Test Management Plan.

#### A.17.9.12 Approve for Implementation

- A.17.9.12.1 The Contractor shall perform changes according to the agreed-upon and validated State change schedule.
- A.17.9.12.2 The Contractor shall participate in the State TCCB meetings and provide subject matter experts as needed to answer questions prior to formal approval process.
- A.17.9.12.3 The Contractor shall update change records within the Change Control Tool with the appropriate status changes and details about the change and communicate updates to State stakeholders and partners.
- A.17.9.12.4 The Contractor shall receive State TCCB approval for all changes prior to promotion into the Production environment.

#### A.17.9.13 Coordinate and Implement

- A.17.9.13.1 The Contractor shall produce and publish to the State ongoing formal documentation of the activities and checkpoints required to coordinate and implement authorized change(s).
- A.17.9.13.2 The Contractor shall provide implementation team members to be on call and available following any implemented changes to production systems.
- A.17.9.13.3 The Contractor shall be able to back out any implemented changes that have a negative impact on the system and return the system and data to its natural state before the change was made.
- A.17.9.13.4 The Contractor shall send notifications to the State's stakeholders pre- and post- change implementation.
- A.17.9.13.5 The Contractor shall communicate and coordinate with the State's Configuration Manager to ensure that all CI changes resulting from a new change is appropriately documented in the Configuration Management Database (CMDB).

#### A.17.9.14 Review and Close

- A.17.9.14.1 The Contractor shall perform a formal post-implementation change review to confirm that the change has met objectives, and that the State's relevant change stakeholders are satisfied with the results. This review shall be based on formal post-implementation change review process, which shall be included in the Contractor's Technology Change Management Plan, and approved by the State.
- A.17.9.14.2 The Contractor shall document and publish to the State, lessons learned to provide an opportunity to improve the Technology Change Management process for future changes.

#### A.17.10 Configuration Management

- A.17.10.1 The Contractor shall be responsible and accountable for the development and management of configuration activities in compliance with existing standards and non-functional architecture requirements.
- A.17.10.2 Configuration Management Plan

- A.17.10.2.1 The Contractor shall create and execute an approved Configuration Management Plan as part of the PMP. Activities include: configuration planning, management of CMDB, CI identification, performing configuration audits, and reporting on configuration performance.
  - A.17.10.2.2 The Contractor's Configuration Management Plan shall integrate with the State's Configuration Management Plan
  - A.17.10.2.3 The Contractor shall purchase, build, and maintain a CMDB that is maintained per the standards defined in the State's Configuration Management Plan. The CMDB shall be maintained within a service management tool that integrates the CMDB with other service management capabilities such as Incident Management and Change Management.
- A.17.10.3 Configuration Items
- A.17.10.3.1 CIs shall be integrated to an enterprise CMDB.
  - A.17.10.3.2 CIs shall be defined by the Contractor in coordination with State business and IS leadership to ensure appropriate level of granularity.
  - A.17.10.3.3 Older versions of approved baseline configurations shall be maintained and made available for review and rollback if needed.
  - A.17.10.3.4 Records of configuration controlled changes to the information system shall be retained for at least three (3) years unless a longer period is mandated by the State.
- A.17.10.4 Control Configuration
- A.17.10.4.1 The Contractor configuration data model shall be consistent with the State's enterprise CMDB configuration data model.
  - A.17.10.4.2 The Contractor shall manage the lifecycle of each CI from identification through retirement.
- A.17.10.5 Monitor Configuration
- A.17.10.5.1 The Contractor shall develop standard reports in coordination with the State which provide views, at a minimum, to the definition of CIs, CI relationships, and status.
  - A.17.10.5.2 Updates to CIs shall be published monthly, unless otherwise stated in the State Configuration Management Plan.
- A.17.10.6 Validate and Verify Configuration
- A.17.10.6.1 The Contractor shall perform periodic audits of the CMDB to ensure accuracy and reliability of data as defined by the State.
  - A.17.10.6.2 The Contractor shall publish findings from CMDB audits in a report and share with the State.

- A.17.10.6.3 The Contractor shall resolve findings from the CMDB audits within thirty (30) days.

#### A.17.11 Release and Deployment Management

- A.17.11.1 The Contractor shall be responsible and accountable for moving releases through the development and initial test environments, as well as the production environment, and coordinating with the State to plan and schedule releases based on the business priorities.

- A.17.11.2 The Contractor shall develop formal release and deployment management processes and procedures to effectively govern the release and deployment management process and ensure all parties are ready for the release.

#### A.17.11.3 Review and Validate Release

- A.17.11.3.1 The Contractor shall provide specifications for industry standard software to automate and manage the versioning/release control for each individual deployment. The Contractor shall provide any/all tools necessary to fulfil the obligations of this contract.

- A.17.11.3.2 The Contractor shall develop and execute a Release and Deployment Management Plan that integrates with the State's Release and Deployment Management Plan.

- A.17.11.3.3 The Contractor shall own and manage the entire Release and Deployment lifecycle in coordination with State stakeholders and other third party providers.

#### A.17.11.4 Release Planning:

- A.17.11.4.1 The Contractor shall develop and perform a formal review process to clearly define and approve the release plans with the State's relevant stakeholders.

- A.17.11.4.2 The Contractor shall assign distinct resources to the deployment process, which are subject to State approval. Access to production and non-production environments shall be restricted based on the Access Control List.

- A.17.11.4.3 The review process shall include project management planning, and configuration management reports on the status of the to-be-deployed-to environment.

#### A.17.11.5 Build and Configure Release:

- A.17.11.5.1 The Contractor shall perform unit tests on each independent component that was built and/or configured.

- A.17.11.5.2 The Contractor shall produce formal documentation of all build notes for all releases including emergency releases. These notes shall be submitted to the State for approval prior to build.

#### A.17.11.6 Test and Accept Release

- A.17.11.6.1 The Contractor shall produce a formal test certificate as part of the release approval process. The Test certificate must follow the process and standards defined within the Test Management Plan.
- A.17.11.6.2 The Contractor shall submit release documentation, including build notes, test results/certificate to the State for acceptance of the release.

A.17.11.7 Deployment Planning:

- A.17.11.7.1 The Contractor shall develop and execute an Implementation and Deployment Plan for all new releases and publish to all relevant IT and Business stakeholders across the State for approval.
- A.17.11.7.2 The Implementation and Deployment Plan shall take into consideration all dependencies and be closely aligned with the State's Change Management Plan.
- A.17.11.7.3 The Contractor shall manage release to the Production environment, which do not conflict with primary business operating and service delivery hours.
- A.17.11.7.4 The Contractor shall communicate to the State's team pre and post-notifications if the deployment involves downtime in the production environment.
- A.17.11.7.5 The Contractor shall include risk and risk mitigation plans, including a back-out approach, for each Release deployment.
- A.17.11.7.6 The Contractor shall develop and manage a formal and documented procedure to ensure the integrity of the release package and its constituent components throughout the transition activities. The procedure shall be published to the State.
- A.17.11.7.7 The Contractor shall communicate each release to the applicable State IS and Business stakeholders following an approved communication plan which shall be detailed within the Release and Deployment Plan.
- A.17.11.7.8 The Contractor shall maintain segregation of duties between development and release management teams.

A.17.11.8 Perform Operational Readiness:

- A.17.11.8.1 The Contractor shall perform formal and documented Operational Readiness validation to ensure there is appropriate knowledge transfer to the users impacted by the new release and the Service Desk that shall be supporting the release. The Operational Readiness validation outputs shall be published to the State for review and approval.

A.17.11.9 Go-Live for Release

- A.17.11.9.1 The Contractor shall manage deployment automation tools to increase efficiency, speed, and accuracy of the release.

- A.17.11.9.2 The Contractor shall dedicate support resources, available at a capacity agreed upon by the State, to determine success of the deployment and resolve any resulting issues.
- A.17.11.9.3 The Contractor shall ensure delivery of pre and post-implementation communication to the designated State personnel resources on all changes implemented into the production environment or any other environment identified by the State.
- A.17.11.9.4 The Contractor shall own maintenance and repair responsibilities for any production issues related to a change implemented into the production environment.

#### A.17.11.10 Manage Warranty Support

- A.17.11.10.1 The Contractor shall develop and manage a formal process to ensure that the new or changed service is capable of delivering the utility and warranty as agreed upon and stated by the State. The process shall be published to the State and signed-off by the State's relevant stakeholders. Additional information can be found in Section A.26.

#### A.17.12 Asset Management

- A.17.12.1 The Contractor shall be responsible and accountable for the identification, installation, maintenance, retirement, and financial tracking activities for the software and hardware assets supporting TEDS.
- A.17.12.2 Request IT software/hardware asset
  - A.17.12.2.1 The Contractor shall be responsible for identifying required software and hardware for TEDS activities. The Contractor shall identify interdependencies between existing assets and associated costs
- A.17.12.3 Procure IT software/hardware
  - A.17.12.3.1 The Contractor shall provide software/hardware specifications, based on approved Capacity Plan and System Configuration documentation, to support the State's procurement of IT assets.
  - A.17.12.3.2 The Contractor shall be responsible for development and maintenance of an Asset Library to enable accurate and up-to-date tracking and monitoring of procured IT software/hardware assets and related versions.
- A.17.12.4 Deploy IT software/hardware assets
  - A.17.12.4.1 The Contractor shall develop and manage a formal software/hardware asset deployment process. The deployment process shall be published to the State for approval.
  - A.17.12.4.2 The Contractor shall be responsible for performing the test suite against the new assets, following the process and standards defined within the Test Management Plan.
- A.17.12.5 Manage IT software/hardware assets

- A.17.12.5.1 The Contractor shall be responsible for implementation and maintenance of all TEDS related software/hardware assets.
- A.17.12.5.2 The Contractor shall be responsible for development and maintenance of an asset management tool(s) to provide the state a complete view of assets lifecycle, usage, regulatory compliance, costs, changes and viability.
- A.17.12.5.3 The Contractor shall log and track assets in parallel with the CMDB.
- A.17.12.5.4 The Contractor shall be prepared for, and participate in, periodic asset audits performed by the State or other State Contractors.

#### A.17.12.6 Decommission/Retire IT Software/Hardware Assets

- A.17.12.6.1 The Contractor shall produce and publish to the State, a formal software/hardware assets replacement, decommission, and retirement process.

#### A.17.13 Event Management

- A.17.13.1 The Contractor shall be responsible for coordinating with the State and STS on the detection, documentation, investigation and determination of corrective actions for events, including but not limited to bottlenecks, degradations delays, response times, anomalies, and any potential event, that can impact the system in a negative or unpredictable manner.
- A.17.13.2 The Contractor shall monitor production 24/7/365.
- A.17.13.3 The Contractor shall maintain 24/7/365 on-site production support team (Service Desk) to identify, monitor, and coordinate TEDS alerts, in cooperation with the State and other service providers.
- A.17.13.4 The Contractor shall develop, or leverage existing tools where available and possible, event management capabilities and tools.
- A.17.13.5 The Contractor shall develop, maintain, and manage a plan to monitor every operation that affects the TEDS (e.g. network, hardware, software, interfaces, services, data manipulation).
- A.17.13.6 Engineer and Configure Event Management System
  - A.17.13.6.1 The Contractor shall produce and maintain formal definitions for commonly occurring events based on industry standards.
  - A.17.13.6.2 The Contractor shall produce, maintain, and enforce formal event handling procedures.
- A.17.13.7 Detect and Log Event
  - A.17.13.7.1 The Contractor shall produce and enforce formal procedures for detection and logging of events.
  - A.17.13.7.2 The Contractor shall produce and maintain event logs in compliance with the State's policies and procedures.

#### A.17.13.8 Correlate and Filter Event

- A.17.13.8.1 The Contractor shall produce formal process and documentation determining filtering definitions, policies, and procedures. The documentation shall be published to the State for approval.
- A.17.13.8.2 The Contractor shall implement fully automated correlation engines for grouping of events. The correlation rules that drive the correlation engines shall be published to the State and continuously reviewed for improvement opportunities.
- A.17.13.8.3 The Contractor shall configure each triage tool to integrate with external service management tools.

#### A.17.13.9 Select Event Response

- A.17.13.9.1 The Contractor shall communicate all events to the approved State stakeholders and partners, within an approved timeframe based on severity of the event.

#### A.17.13.10 Review and Close Event

- A.17.13.10.1 The Contractor shall develop and manage a formal event review process. The process and the findings must be published to the State.
- A.17.13.10.2 The Contractor shall log corrective actions and close out event with State approval.

#### A.17.14 Incident/Problem Management

- A.17.14.1 The Contractor shall be responsible for maintaining a 24/7/365 on-site production support team (Service Desk) to coordinate incident identification, investigation, and diagnosis in cooperation with the State and other service providers.
  - A.17.14.1.1 The Contractor shall supply dedicated resources to perform Incident Management activities.
  - A.17.14.1.2 The Contractor shall manage and maintain a tool that enables State have complete access into the incident management process.
  - A.17.14.1.3 The Contractor shall develop, or leverage existing tools where available and possible, incident management capabilities and tools.

#### A.17.14.2 Interaction Handling

- A.17.14.2.1 The Contractor shall develop, execute, and manage an Incident Management Plan, which shall be approved by the State.
- A.17.14.2.2 The Contractor's Incident Management Plan shall integrate with existing State and other third party processes.
- A.17.14.2.3 The Contractor shall outline their monitoring/alerting procedures within the Incident Management Plan that addresses but is not limited to the following:

- a) Alerting capability on any and all hardware, systems, applications, and access points
- b) Identifying errors in processing input files and/or output files. This alerting system shall capture errors in the interface application(s)
- c) Communication guidelines that include escalation procedures
- d) Root cause analysis with development of action plans and implementation of solution/workaround
- e) Process for resolving production issues

#### A.17.14.3 Record, Classify, Prioritize

A.17.14.3.1 The Contractor shall be responsible for detecting, recording, classifying, and prioritizing incidents. Incident prioritization shall be approved by the State.

A.17.14.3.2 The Contractor shall address the procedures and standards for handling problems within Incident Management Plan.

#### A.17.14.4 Investigation and Diagnosis

A.17.14.4.1 The Contractor shall be responsible for investigating and diagnosing incidents. All procedures and findings shall be documented in an incident management tool and visible to the State.

A.17.14.4.2 The Contractor shall perform root cause analysis for all incidents and communicate the findings to the State, the CIP Manager, and other State Contractors. Root cause analysis identifies those incidents that:

- a) Could have been caught
- b) Should have been caught
- c) Would not have been caught, and
- d) Provides a Mitigation Plan for incident.

A.17.14.4.3 Security and privacy incidents shall be reported to State Privacy and Security Offices as soon as possible, but no more than twenty four (24) hours from awareness of the incident or sooner if overriding regulations apply.

#### A.17.14.5 Resolution & Recovery

A.17.14.5.1 The Contractor shall be responsible for identifying and enacting resolutions to incidents. In cases where a permanent resolution is not currently available, a temporary work around must be provided by the Contractor.

A.17.14.5.2 The Contractor shall be responsible for validating that the incident has been resolved and that the resolution meets the needs of the end user.

#### A.17.14.6 Closure

- A.17.14.6.1 The Contractor shall develop, manage, and adhere to incident closure procedures.

#### A.17.15 Request Management

##### A.17.15.1 Initiate Request

- A.17.15.1.1 The Contractor shall be responsible for identifying needs to support TEDS and initiating, classifying, and fulfilling requests. The Contractor shall be required to create a justification case for each request and submit to the State for approval.

##### A.17.15.2 Validate & Classify Request

- A.17.15.2.1 The Contractor shall provide and manage a tool for logging, recording, and categorizing requests.
- A.17.15.2.2 The Contractor shall develop procedures and criteria for validating and classifying requests.
- A.17.15.2.3 The Contractor shall use categorization and trending to identify possible training issues or areas for improving the end user experience in the TEDS.

##### A.17.15.3 Evaluate Request

- A.17.15.3.1 The Contractor shall communicate requests to the State for evaluation and approval.

##### A.17.15.4 Fulfill Request

- A.17.15.4.1 Once request is approved by State leadership, the Contractor shall fulfill requests in accordance with State standards.

##### A.17.15.5 Review & Close Request

- A.17.15.5.1 The Contractor shall validate the request has been fulfilled and meets the needs of the end-user.
- A.17.15.5.2 Once the end-user validates the request has been fulfilled, the Contractor shall be responsible for closing out request.

##### A.17.15.6 Cancel Request

- A.17.15.6.1 The Contractor shall produce and publish to the State a formal request cancelation document.

#### A.17.16 Technology Operations

- A.17.16.1 The Contractor shall maintain a 24/7/365 on-site production control/operations control/console management (Service Desk) providing support to STS and the State for all technology operations activities. All data management activities are to be in compliance with State requirements.

- A.17.16.2 The Contractor shall manage all operation production and output management activities and staff.
- A.17.16.3 The Contractor shall work with HCFA IS managers, STS, Technical Change Control Board, Problem/Incident management and other State Agencies and business partners (i.e. Department of Labor, DHS, Department of Health, Finance and Administration, Axis Direct, Federal Hub, CMS, Hewlett Packard, etc.)
- A.17.16.4 The Contractor shall manage any/all real time transactions, batch scheduling, output/print (i.e. notices, letters), interfaces, changes, and other production/operational related issues and activities.
- A.17.16.5 The Contractor shall develop and provide a daily Operations Report, including, but not limited to:
  - A.17.16.5.1 Interface events and issues
  - A.17.16.5.2 System events and issues
  - A.17.16.5.3 Software events and issues
  - A.17.16.5.4 Errors and Anomalies
  - A.17.16.5.5 Transactions Sent and Received (Daily and Total Amount)
  - A.17.16.5.6 Transaction Types
  - A.17.16.5.7 Staffing and Operational Activities and Issues
  - A.17.16.5.8 Number of notices and letters received and sent (including any and all reconciliation efforts)
  - A.17.16.5.9 Audit tracking of letter/notices by page
  - A.17.16.5.10 Cumulative statistics and complete breakdown of all letters and notices by type.
  - A.17.16.5.11 Performance against Service Levels Agreements
  - A.17.16.5.12 Such other information as the State may request in writing from the Contractor.
- A.17.16.6 Service Desk
  - A.17.16.6.1 The Contractor shall maintain a 24/7/365 Service Desk partnering with STS and the State to resolve issues.
  - A.17.16.6.2 The Contractor shall leverage existing Server and Hardware Management tools and processes when possible within the STS NOC.
  - A.17.16.6.3 The Contractor shall maintain a 24/7/365 Service Center within the Service Desk in close coordination with the infrastructure service provider (STS).

- A.17.16.6.4 The Contractor shall leverage existing tools and processes used in the STS NOC where available and possible.
- A.17.16.6.5 The Contractor shall maintain 24/7/365 console management strategies within the Service Desk providing support to the State.
- A.17.16.6.6 The Contractor shall review TEDS batch job requests, validate schedules, and coordinate computer processing time based on system priorities, program run-time, processing, and restart requirements; considering batch and production windows/schedules.
- A.17.16.6.7 The Contractor shall maintain 24/7/365 Online and Batch Job management procedures within the Service Desk.
- A.17.16.6.8 The Contractor shall provide any/all scheduling information and monitoring tools to meet the requirements of this contract.

#### A.17.16.7 Backup and Restore

- A.17.16.7.1 The Contractor shall develop and maintain State-approved backup and restore process and documented procedures to support State technical teams through the SDLC process.
- A.17.16.7.2 The Contractor shall provide backup and restore completion reports to the State for review during periodic service level review meetings.
- A.17.16.7.3 The Contractor shall perform a State-selected data restore test on a monthly basis that demonstrates successful backup/recovery strategies.
- A.17.16.7.4 The Contractor shall maintain the Solution's Recovery Time Objective (RTO) of two (2) hours. In case of a disaster that affects system operations, the Solution shall be restored in its entirety within two (2) hours.
- A.17.16.7.5 The Contractor shall maintain the Solution's Recovery Point Objective (RPO) of no more than one (1) hour of data loss. In case of a disaster that affects the system operations, a maximum of one (1) hour of data inputs to the Solution may be lost and require re-entry.

#### A.17.16.8 Storage and Archive

- A.17.16.8.1 The Contractor shall comply with the storage archiving and purging policies and procedures established by the State.

#### A.17.16.9 Network Management

- A.17.16.9.1 The Contractor shall partner and leverage existing Network Management tools and processes within the STS NOC.

#### A.17.16.10 Database Administration

- A.17.16.10.1 The Contractor shall monitor the Database performance and operations on 24/7/365 basis.

A.17.16.10.2 The Contractor shall be responsible for any/all application and database functions, including but not limited to: maintaining product currency (version/release/patching), security, licenses, file maintenance, tuning, optimization, and all related Database Administration functions.

#### A.17.16.11 Directory Services Management

A.17.16.11.1 The Contractor shall develop a Solution that is compatible with the State's Directory Services and Identity Management solution.

A.17.16.11.2 The Contractor, in coordination with STS and the State, shall monitor events 24/7/365 on the Directory Services, such as unsuccessful attempts to access a resource, and take the appropriate action where required.

#### A.17.16.12 Middleware (Application/Internet/Web) Management

A.17.16.12.1 The Contractor, in coordination with the State and other State Contractors function, shall ensure that appropriate middleware solutions for the TEDS are chosen and that they can perform optimally when they are deployed.

A.17.16.12.2 The Contractor, in coordination with STS, shall detect and resolve issues related to TEDS middleware.

A.17.16.12.3 The Contractor, in coordination with STS, shall update TEDS-related middleware, including licensing, patching, and installing new versions.

#### A.17.16.13 Facilities and Data Center Management

A.17.16.13.1 The Contractor shall comply with the existing processes and standards for Data Center Management provided by STS, and leverage STS services for maintaining the TEDS infrastructure.

#### A.17.17 Print Output Management

##### A.17.17.1 Print/Letter/Notices/Electronic Output

A.17.17.1.1 The Contractor shall be responsible for the TEDS print output (letters/notices) that shall be stored as individual electronic documents in an electronic content management system, indexed and associated to existing application/case/member, archived, and available for viewing and/or printing through the TEDS.

A.17.17.1.2 The Contractor shall define, develop, implement, and maintain a document management system (e.g. HP Exstream) for managing all aspects of document creation, modification, and output.

A.17.17.1.3 The Contractor shall define, develop, implement, and maintain an electronic content management system. The State shall like to re-use, where possible, the currently utilized ECM tool, FileNET.

- A.17.17.1.4 The Contractor shall be responsible for creating, processing, printing, mailing and tracking each mail piece through the output process. Output management includes, but is not limited to, forms design, printing, folding/insertion into envelopes, co-mingling, and delivery to the USPS.
- A.17.17.1.5 The Contractor shall manage and re-mail returned mail received from the USPS, and associating to an existing application/case/member.
- A.17.17.1.6 The Contractor shall systematically update addresses received from the USPS as directed by the State.
- A.17.17.1.7 The Contractor shall provide and maintain approved inventory levels, including mailing envelopes and attachments as necessary.
- A.17.17.1.8 The Contractor shall support USPS tracking processes and industry standard print tracking processes, including but not limited to intelligent mail barcode and USPS address verification and validation. Examples of USPS address verification and validation systems include:
- a) Coding Accuracy Support System
  - b) Multi-line Accuracy Support System
- A.17.17.1.9 The Contractor shall provide complete tracking of each individual letter/notice by page and provide a complete audit of such in the Daily Operations Report.
- A.17.17.1.10 The Contractor shall produce, print, and mail all printed output.
- a) Routine TEDS letters and notices that are to be printed, shall be inserted and mailed within two (2) business days of production, as defined by the State's daily operation processes.
  - b) The Contractor shall have the ability to future date TEDS letters and notices.
  - c) High-volume or mass mailing of TEDS letters and notices that are to be printed, shall be inserted and mailed based on a schedule defined by the State's operation processes.
- A.17.17.1.11 The Contractor shall deliver the letter/notice to the USPS within two (2) business days of letter creation.
- A.17.17.1.12 The Contractor shall provide postage mechanisms and be responsible for all postage costs to be utilized during the output process.
- A.17.17.1.13 The Contractor shall archive and store the combined bulk print-stream for audit and review purposes.
- A.17.17.1.14 The Contractor shall be directly responsible for ensuring all notices, letters and other electronically generated output is produced, printed, mailed and thoroughly monitored for completeness and quality.

- A.17.17.1.15 The Contractor shall manage, on a daily basis, the relationship with any/all third-party service providers to manage and resolve any issues associated with print output.
  - A.17.17.1.16 The Contractor shall provide a test environment to ensure all development, including forms (template) design, content, data accuracy and through-put is thoroughly tested and approved by the State before moving into production.
  - A.17.17.1.17 The Contractor shall have the ability to print all documentation in a double-sided format and in Spanish if required by the State.
  - A.17.17.1.18 The Contractor shall process, print, and mail documents in the appropriate envelope as defined by number of pages and envelope size limitations.
  - A.17.17.1.19 The Contractor shall ensure that all notices are formatted to align the letter or notice address with USPS envelope address windows, and prevent all other information from being visible.
  - A.17.17.1.20 The Contractor shall have the ability to include attachments or inserts, which vary by notice type, within the printing process.
  - A.17.17.1.21 The Contractor shall have the ability to print letters, notices, and attachments on color pages, as defined by the State.
  - A.17.17.1.22 The Contractor shall ensure that notice-related errors triggered during the batch-print process do not prevent the completion of the batch-print process.
  - A.17.17.1.23 The Contractor shall have the ability to perform high-volume batch printing in one session or separated across multiple sessions. The Contractor shall provide the printers needed for this functionality at no additional cost to the State and to be located at the Contractor's facility.
  - A.17.17.1.24 The Contractor shall provide manual work-around processes, at no additional cost to the State, upon failure of automated output processes.
- A.17.17.2 Document Print/Letter/Notices/Electronic Output Management
- A.17.17.2.1 The Contractor shall provide on-going support, testing, and maintenance of the Output Management Software for print, notices, letters, and templates.
  - A.17.17.2.2 The Contractor shall create and/or modify specified print, notice, letter templates, and other elements within time frames specified by the State. The list of notices can be found in Contract Attachment 3.
  - A.17.17.2.3 The Contractor shall provide test environment and drafts for approval by State business unit and business partners. The Contractor shall include the State throughout the lifecycle of notice development and testing.
  - A.17.17.2.4 The Contractor shall, upon State approval, deploy new or modified templates and print/letters to production environment.

- A.17.17.2.5 The Contractor shall set-up, execute, monitor, and take corrective action on any/all issues related to print, notices, letters, and production/test processes.
- A.17.17.2.6 The Contractor shall work with State agencies and/or third party mail vendors, mail co-mingle vendors, and other State partners to track the quantity and quality of each type of print, notice, or letter created as part of the daily processing cycle by the TEDS.
- A.17.17.2.7 The Contractor shall take corrective action to resolve all production discrepancies, issues, and incidents before errors reach the USPS.
- A.17.17.2.8 The Contractor shall regenerate print data files as requested.
- A.17.17.2.9 The Contractor shall monitor and review all print, notice, or letter file outputs for completeness and ensure the correct print, notice, or letter is generated for the intended purpose and the intended recipient.
- A.17.17.2.10 The Contractor shall reconcile any discrepancies/differences and take corrective action before progressing to the next step.
- A.17.17.2.11 The Contractor shall compare counts of each printed notice/letter type generated in TEDS with folder/inserters and USPS counts in real-time to prevent any lost, incomplete or overage in production.
- A.17.17.2.12 The Contractor shall produce and reconcile final counts of each print, notice and letter type to validate postage charges and send final report to the State daily.
- A.17.17.2.13 The Contractor shall test new or modified print, letters and notices to ensure quality and accuracy of templates.
- A.17.17.2.14 The Contractor shall monitor daily print, validate quality, process letters and notices and accommodate necessary changes to the daily print, letter, and notices schedule based on outages, ad-hoc requests, or needed system recoveries.
- A.17.17.2.15 The Contractor shall design, develop, manage and practice letter and notice processing portion of the BC/DR Plan for letter and notice processing.
- A.17.17.2.16 The Contractor shall provide proof of services and evidence of a contract for a disaster recovery site for Print Output Management.
- A.17.17.2.17 The Contractor shall develop and establish a program of regular DR testing, at a minimum twice a year, to ensure critical components of the BC/DR strategy can be recovered within the desired Recovery Time Objective for Print Output Management.

#### A.18 Turnover

- A.18.1 The Contractor shall be responsible for planning and supporting turnover of the Solution at the completion of the required term, or in the event of contract termination. The Contractor shall provide a complete transition to a successor, which could include the State or other State contractors. The State may exercise an option to extend the

Operations and Maintenance period of this Contract and delay all Turnover activities for a commensurate period of time. The State shall work closely with the Contractor during this process and must approve all updates to the Contractors Turnover approach and plans.

A.18.2 The Contractor shall maintain staff throughout the Turnover period to satisfy and maintain compliance with all performance standards and requirements identified in the Contract. The Contractor shall supply additional staff on-call for three (3) months after the successful Cut-Over. Turnover activities include:

- A.18.2.1 Planning for the Turnover
- A.18.2.2 Managing and Executing the Turnover
- A.18.2.3 Turnover Training and Knowledge Transfer
- A.18.2.4 Cut-Over
- A.18.2.5 Contract Closeout

A.18.3 Planning For The Turnover

A.18.3.1 The Contractor shall develop, deliver, and execute a Turnover Plan. The Turnover Plan shall include a comprehensive approach to turnover, including but not limited to resources, staffing, training, milestones, and tasks to successfully transfer responsibility for Operations and Maintenance of the Solution at a level of performance and customer support equal to the level achieved by the Contractor. The Turnover Plan shall include:

- A.18.3.1.1 Procedures to identify all software, data, documentation, and miscellaneous supplies that shall be transferred to the State
- A.18.3.1.2 Approach to how the Contractor shall support training and knowledge transfer from the Contractor to the State
- A.18.3.1.3 Approach to testing and verification, consistent with agreed upon testing procedures with the State
- A.18.3.1.4 Approach to cut-over of the Service Desk, which can occur either concurrent with or after the system cut-over at the discretion of the State
- A.18.3.1.5 Success criteria for the completion of cut-over and final acceptance of all Operations and Maintenance service activity, including defect resolution, by the State
- A.18.3.1.6 Mitigation and CPs to address turnover failures
- A.18.3.1.7 State and Contractor tasks for Turnover
- A.18.3.1.8 Schedule for Turnover
- A.18.3.1.9 Approach to verification of the States readiness, including assessments of staff, technology, and processes
- A.18.3.1.10 Approach to managing change to the Solution throughout the transition

#### A.18.4 Managing And Executing The Turnover

- A.18.4.1 The Contractor shall provide consistent staffing, including Key Personnel and management, during the execution of the Turnover to transition all aspects of operation of the Solution from the Contractor to the State or other State Contractors. The Contractor and State shall confirm transition to the successor.

#### A.18.5 Management of the Turnover

- A.18.5.1 The management of the Turnover shall be integrated with the project management structure and successor's schedule. The primary activities in this stage are focused on transition planning to support the continuation of operational readiness of the TEDS. The Contractor shall manage all aspects of the Turnover that affect cost, schedule, performance (scope and quality), risk/issues/opportunities, and resources that are under Contractor control. Additionally, the Contractor shall work with the State and/or successor to implement the Turnover Plan.
- A.18.5.2 The Contractor shall prepare, in cooperation with the Successor, and submit a Turnover schedule within six (6) months or one hundred twenty (120) business days (whichever is longer), of the State's informing the Contractor of the start of the turnover stage. The schedule shall address all Turnover activities until the successful transition of operations.

#### A.18.6 Staffing the Turnover

- A.18.6.1 The Contractor shall have an organizational staffing model in place to retain appropriate staffing levels for the successful continuation of operations, and to support the transition during the Turnover stage. The Contractor shall have staff to successfully support all requirements of the Contract until Contract closeout is finalized.
- A.18.6.2 The staffing model shall include an estimate of the types of skills, responsibilities, and salary of personnel required to assume full Operations and Maintenance support as delivered by the Contractor under this Contract.
- A.18.6.3 The staffing model shall include both the type of activity of the personnel and the location of the personnel, including but not limited to the following activities:
- A.18.6.3.1 Application Management Operations and Maintenance functions
  - A.18.6.3.2 Technical Management Operations and Maintenance functions
  - A.18.6.3.3 Systems, Network, Database, and Storage Management functions
  - A.18.6.3.4 Service Desk Operations and Maintenance functions
  - A.18.6.3.5 Administrative Staff
  - A.18.6.3.6 Management
  - A.18.6.3.7 Other Key Contacts

#### A.18.7 Executing the Turnover

- A.18.7.1 The Contractor shall execute the Turnover to transition all aspects of operation of the Solution to the State or identified party. This includes the transfer of software, including source program code, COTS systems, and executable copy of the enhanced Solution, and all related system and process documentation. The Contractor shall ensure that all transferred information is current as of the last successfully implemented change.
- A.18.7.2 Throughout the Turnover the Contractor shall work with the State to coordinate system change activities, define a freeze period, and develop a process for implementation and coordination of any emergency change required during the execution. All transfers must be made on electronic media or network transfer and approved by the State.
- A.18.7.3 At a minimum, the Turnover shall include the Contractor providing the following items and support:
  - A.18.7.3.1 Inventory and configuration of all hardware/system components required to support Operations and Maintenance for all environments of the Solution at the required level of performance, availability, and capacity, including:
  - A.18.7.3.2 As-Is hardware configuration diagrams showing the relationship between all system, network, security, and service management components
  - A.18.7.3.3 All System hardware/firmware descriptions, licenses, versions/releases
  - A.18.7.3.4 All security management, service management, storage management, code management, and test management software
  - A.18.7.3.5 Inventory of all software, data and associated documentation to be transferred
  - A.18.7.3.6 All source code, complied code, scripts
  - A.18.7.3.7 All System software/firmware descriptions, licenses, versions/release
  - A.18.7.3.8 Inventory of all development, Operations and Maintenance tools, processes and procedures in use by the Contractor in support of the Solution.
  - A.18.7.3.9 Inventory of all tools and documentation used by the Service Desk
  - A.18.7.3.10 Proof of licensing and maintenance contracts for all purchased software components
  - A.18.7.3.11 BC/DR site requirements
  - A.18.7.3.12 Periodic transfers of all software, file systems and documentation
  - A.18.7.3.13 Transfer and verification of all user ID and access information to include all configuration data and documentation in use to be establish and maintain accurate user access

- A.18.7.3.14 Verification that documentation, including user, functional, maintenance, development and operational manuals needed to operate and maintain the system is available in electronic format
- A.18.7.3.15 Transfer of all current and historical support records including but not limited to:
  - a) Incident Management Records
  - b) Problem Management records including work-around(s) and known errors or defects
  - c) Change Management records, including Post Implementation reports
  - d) Release Management records
  - e) Security Incident records
  - f) System and Network performance reports
  - g) System and Network performance data records
  - h) Root Cause Analysis reports
- A.18.7.3.16 Assist the State in validating and verifying all systems are appropriately configured, and support incident response, system restoration, problem identification and problem resolution throughout all stand-up and testing activity
- A.18.7.3.17 Participate with the State in execution of all testing
- A.18.7.3.18 Completion of the State readiness assessment to include assessment of ability of technology, personnel and processes to support full Solution Operations and Maintenance at the level of performance established by the State

#### A.18.8 Turnover Training and Knowledge Transfer

- A.18.8.1 The Contractor shall provide training to the State staff and/or the successor Contractor for no less than 6 months prior to cut-over in order for the State to assume responsibility of the O&M of the Solution. The contractor shall augment training with mentoring and shadowing of personnel either in the Contractor's production environment or during set-up and testing of the States environments.
- A.18.8.2 At a minimum, the Turnover training shall include the following:
  - A.18.8.2.1 Introduction to the Solution functions and capabilities
  - A.18.8.2.2 All application development tools, processes, and procedures
  - A.18.8.2.3 All application (custom or COTS)/system/infrastructure Operations and Maintenance responsibilities
  - A.18.8.2.4 All application/system/infrastructure support processes and procedures

A.18.8.2.5 All management tools (e.g., security management, systems management, storage management, IT service management, etc.)

A.18.8.2.6 All Service Desk systems, processes, and procedures

A.18.8.2.7 Any and all other responsibilities necessary to sustain Operations and Maintenance of the Solution at the required level of performance

A.18.8.2.8 Standard Operating Procedure manual

#### A.18.9 Contract Closeout

A.18.9.1 Contract closeout occurs at the end of the Turnover stage. The State expects the Contractor to have completed all contracted work during the Operations stage prior to contract closeout. Any incomplete or remaining work in which the Contractor expects to transition to the State or successor Contractor must receive prior approval from the State. Contract closeout responsibilities, deliverables and penalties shall survive the termination date of this Contract and continue until the Contractor has fulfilled all Turnover activities and met all closeout requirements to the State's satisfaction and approval. The Contractor shall provide verification in writing to the State that all items required to be transferred to the State have been transferred and removed from the Contractors systems. The verification in writing shall be delivered to the State at a date before the end of the Turnover period as determined by the State.

#### A.19 Security and Privacy

A.19.1 The Contractor shall, for any and all systems involved in the processing of the Patient Protection and Affordable Care Act (PPACA) and HIPAA related information, comply with the all applicable Federal and State laws and regulations as required for each data type and classification.

A.19.1.1 Any reference to MARS-E, even under CMS context references, should also infer compliance with current IRS Safeguards Program and IRS Publication 1075, including future updates, where applicable by usage of data type and/or classification.

A.19.2 The Contractor shall ensure capabilities are provided in their system design to support CMS guidance issued in the "NIST Special Publication 800-63-2", including future CMS updates.

A.19.3 The Contractor shall develop a FTI labeling methodology, included within the System Architecture Design Document, for any location in which IRS data will be stored. This shall be approved by the HCFA Privacy Office. IRS data shall be grouped together as much as possible by design to prevent comingling.

A.19.4 The Contractor shall be responsible for the following phases with regards to security and privacy related activities throughout the lifecycle of the contract under the oversight of the State:

A.19.4.1 DDI

A.19.4.2 Operations and Maintenance

A.19.4.3 Testing

- A.19.4.4 Monitoring
- A.19.5 The Contractor shall ensure that all file uploads from remote users in the Solution shall have a virus scan prior to being processed further with appropriate feedback to the uploader of success or failure.
- A.19.6 Data Classification
  - A.19.6.1 The Contractor shall classify all data collected by the Solution, regardless of the source (such as data entered through the web portal, data received through interfaces from sources such as the FDSH, image scans, Department of Homeland Security, IRS, or file uploads). The State shall approve the security and privacy standards that shall be applied to each classification.
  - A.19.6.2 The Contractor shall identify why and how each data element is captured, how it is to be retained, and the archive and purge processes that apply to the data.
  - A.19.6.3 Contractor shall retain records as required by applicable laws and regulations.
  - A.19.6.4 The Contractor shall classify data elements in a way that identifies applicable security controls based on the Federal and State regulations and policies to the class of the data elements.
  - A.19.6.5 The Contractor shall identify the security controls that apply to each data class and/or type and ensure appropriate controls are established for the Solution based on data flows through the system.
  - A.19.6.6 The Contractor shall maintain and track data types/classifications in the data dictionary or equivalent process.
  - A.19.6.7 The Contractor shall have the ability to provide data classifications for all data extracted from the Solution.
- A.19.7 Regulatory compliance
  - A.19.7.1 The Contractor shall demonstrate that the Solution meets or exceeds industry standards and applicable federal and state security requirements.
  - A.19.7.2 The Contractor shall ensure the security of the Solution is compliant with state and federal standards, regulations and publications, including but not limited to:
    - A.19.7.2.1 45 Code of Federal Regulations (CFR) Part 95.621(f) Automatic Data Processing System Security Requirements and Review Process
    - A.19.7.2.2 NIST Special Publication 800 series
    - A.19.7.2.3 NIST Cryptographic Module Validation List (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>)
    - A.19.7.2.4 IRS Safeguards Program and IRS Publication 1075
    - A.19.7.2.5 Federal Records Retention Schedule 44 USC 3303a
    - A.19.7.2.6 Privacy Act of 1974 at 5 USC 552a

- A.19.7.2.7 Computer Matching and Privacy Protection Act of 1988 (CMPPA)
- A.19.7.2.8 SSA Information System Security Guidelines for Federal, State, and Local Agencies
- A.19.7.2.9 Child Online Privacy Protection Act
- A.19.7.2.10 Medicaid Confidentiality Rules at 42 CFR
- A.19.7.2.11 HIPAA
- A.19.7.2.12 Federal security and privacy standards adopted by the U.S. Department of Health and Human Services for Exchanges (MARS-E)
- A.19.7.2.13 18 USC 1905 Criminal Code: Disclosure of Confidential Information
- A.19.7.2.14 HITECH
- A.19.7.2.15 Patient Protection and Affordable Care Act and U.S. Department of Health and Human Services (HHS) Final Rule
- A.19.7.2.16 Governing State Agency Policies and regulations including State and STS

- A.19.7.3 Once established, no security provisions for firewalls, client and server computers, and user profiles and controls shall be modified without written State approval.

#### A.19.8 Security controls

- A.19.8.1 The Contractor shall be responsible for design, development, implementation, documentation and operation of security controls over access to sensitive functions and data of the Solution until termination of the contract. Security controls include, but are not limited to:

- A.19.8.1.1 Processes and procedures
- A.19.8.1.2 Tools
- A.19.8.1.3 Incident monitoring and response that is compliant with MARS-E
- A.19.8.1.4 CMS, IRS and SSA continuous monitoring and incident reporting directives.

- A.19.8.2 The Contractor shall map security controls and standards established in MARS-E and relevant CMS and IRS guidance to requirements for development and operational processes and procedures.

#### A.19.9 SDLC-related Security Requirements

- A.19.9.1 The Contractor shall prepare and submit artifacts related to security that shall be reviewed in Gate Reviews, as defined in the SDLC, and approved by stakeholders before development may continue.
- A.19.9.2 The Contractor shall prepare architecture artifacts, deliverables and Gate Review documents as specified in the Table of Deliverables in Section A.27.

- A.19.9.3 The Contractor shall resolve any findings identified from a vulnerability assessment.
- A.19.10 Operations and Maintenance-related Security Requirements
- A.19.10.1 The Contractor shall report data breaches to HCFA Privacy, IS Director, and Security offices as soon as possible, but no more than twenty four (24) hours from awareness of the incident or sooner if overriding regulations apply.
- A.19.11 Facilities-related Security Requirements
- A.19.11.1 The Contractor's facilities designated to the project shall meet or exceed all applicable information security and privacy regulations and policies pursuant to the data classifications contained, stored, or in transit within the facilities.
  - A.19.11.2 The Contractor shall be responsible for notifying The State of any data in the facilities (electronic, paper, or other) that is not classified as public and related to State concerns for security and privacy.
  - A.19.11.3 The Contractor shall make its facilities reasonably available for inspection by the State or security staff when requested.
- A.19.12 Continuous Monitoring for Changes to Security and Policy
- A.19.12.1 The Contractor shall monitor Federal (CMS, IRS and SSA at a minimum) and State security policies and regulations as well as those of the States departments and offices including, but not limited to, STS, HCFA, Defense Information Systems Agency, and Security Technical Implementation Guides for system hardening.
  - A.19.12.2 The Contractor shall define in the System Security Plan the approach to monitor, analyze and implement any such changes to the State.
- A.19.13 Coordination with Third-Party Vendors
- A.19.13.1 The Contractor shall be responsible for ensuring that security and privacy policies, processes, procedures and appropriate documentation related to the project environment is satisfactory or identified as a gap for remediation and escalated/tracked, as appropriate.
  - A.19.13.2 The Contractor shall, with regards to the TEDS, perform regular monitoring and assessment of compliance with security and privacy policies, processes, procedures and documentation for all those who access the system, as defined by the State.
- A.19.14 Risk Management Framework
- A.19.14.1 The Contractor shall employ a Risk Management Framework consistent and aligned with the most recent version of the NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, to ensure that throughout all Gates Reviews and O&M:
    - A.19.14.1.1 Information system security related risks are managed in a way that is consistent with the organization's mission/business objectives and overall risk management strategy established by the senior leadership through the risk executive (function);

- A.19.14.1.2 Information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and System Development Lifecycle (SDLC) processes;
- A.19.14.1.3 The framework supports consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity;
- A.19.14.1.4 Information and information systems are effectively secured by implementation of appropriate risk mitigation strategies.

## A.20 Organizational Change Management and Training

- A.20.1 The Contractor shall adhere to and support the implementation of the State's OCMT Approach, and work directly with the OCMT Team for all identified communication and stakeholder engagement needs. The Contractor shall be identified as a Subject Matter Authority in the OCMT Approach and shall assist in the execution of any and all sections, activities, and/or policies per the State-approved OCMT Approach.
- A.20.2 The Contractor shall follow timeline milestones that are representative of the required sequence and timing of activities. Timelines are dependent upon several factors, and the State reserves the right to adjust timelines and sequences of training events based on number of users, availability of training facilities, and the determined combination of instructor-led training and/or self-paced, web-based training learning. Timeline requirements include but are not limited to:
  - A.20.2.1 Training delivery shall begin no fewer than two (2) months prior to each release and remain open for no fewer than one (1) month after each release, as required by the State
  - A.20.2.2 Training environment shall be established and access granted to the OCMT team no fewer than seven (7) months prior to each phase release such that the development of all requisite training materials may begin.
  - A.20.2.3 In accordance with the establishment of the training environment, the Contractor shall provide system training to the OCMT personnel for the purpose of training materials development.
    - A.20.2.3.1 System training shall occur six (6) months prior to Go-Live of the TEDS.
  - A.20.2.4 Training environment refreshes shall be completed at least daily during single-day training delivery and as needed during multi-day training delivery.
- A.20.3 In accordance with objectives of the OCMT Approach and the requirements defined below, the Contractor shall fully comply with all responsibilities and/or perform all activities as a contributing group that supports the successful execution of OCMT.
  - A.20.3.1 The Contractor shall provide subject matter experts for training activities.
  - A.20.3.2 The Contractor shall develop materials and facilitate train-the-trainer sessions.
  - A.20.3.3 The Contractor shall develop and maintain the TEDS training environment.
  - A.20.3.4 The Contractor shall perform data setup activities for the TEDS training environment.

- A.20.4 The Contractor shall include, consult, and work directly with assigned project OCMT personnel for any and all process, systems, and/or operating model planning, analysis, and/or design efforts, workshops, and/or other meetings
- A.20.5 The Contractor shall provide the project plan and validate major milestones and timing to ensure alignment with Stakeholder and/or OCMT activities across the project lifecycle
- A.20.6 The Contractor shall provide process flows (end-to-end processes), including application process steps and systems documentation (including screen shots) to the OCMT team that can be utilized as the foundation to build MMP related trainings
- A.20.7 The Contractor shall provide resources sufficient in any quantity and capability as deemed reasonable by the State to support the following training activities, including but not limited to:
  - A.20.7.1 All those activities defined to support the various phases of the Training Approach (Analysis, Design, Development, Implementation, and Evaluate) that are included in subsequent sections of this document
  - A.20.7.2 Defining user roles
  - A.20.7.3 Supporting the identification of appropriate curriculum and delivery models
  - A.20.7.4 Participating and providing information during Training Development Knowledge Share Sessions
  - A.20.7.5 Validating and approving training materials related to the technical Solution
  - A.20.7.6 Building and maintaining the training environments
  - A.20.7.7 Creation of user profiles and log-in credentials in any quantity as requested by the State to allow trainers and end users appropriate access to the training environments
  - A.20.7.8 Providing subject matter experts in specific work areas, processes, applications, etc. to support classroom learning and train-the-trainer programs supplying at least one (1) SME in each discreet classroom training event
  - A.20.7.9 Providing support of post Go-Live training events that encompass prior training support activities delivered or supported by the Contractor for a period of time as deemed reasonable by the State
  - A.20.7.10 The Contractor shall support the training analysis phase or process by providing and collaborating with the OCMT Team on an ongoing basis in the following ways, including but not limited to:
    - A.20.7.10.1 Providing insight into role definitions and assignments required to operate and/or support future-state applications and processes
    - A.20.7.10.2 Providing insight into standard training curriculum requirements required to support future-state applications and processes
    - A.20.7.10.3 Providing insights into the training delivery framework required to support future-state applications and processes

- A.20.7.10.4 Actively collaborating with training team to select industry standard training approaches for the State end user population
- A.20.8 The Contractor shall build and maintain two (2) fully functional training environments per concurrent release representative of the final-state operational system (e.g., final user interface/GUI) that are dedicated to supporting training activities (training development and training delivery). The two (2) separate environments must clearly and accurately reflect upcoming software versions and closely align with the software release schedule.
- A.20.9 Training development and training delivery environments shall include a minimum of the following:
  - A.20.9.1 Transactional data (masked according to the security and/or confidentiality guidelines provided by the State)
  - A.20.9.2 Training development environment to stage scenarios, get screen shots, etc., to support the defined training schedule
  - A.20.9.3 Identification and provision of training environment data in order to provide for scenario based training
  - A.20.9.4 Specific trainer profiles & credentials that provide fully functional capabilities within both the development and delivery environments
  - A.20.9.5 Sufficient user profiles respective of future state roles within the State to perform and execute any and all potential concurrent classes as defined by the training schedule and/or the State
  - A.20.9.6 Associated log in credentials to support user profiles
  - A.20.9.7 Training environment shall be established and access granted to the OCMT Team no fewer than seven (7) months prior to Go-Live of each release to allow the development of all requisite training materials.
  - A.20.9.8 Training environment shall be established and access granted to end-users no fewer than three (3) months prior to Go-Live of each release.
- A.20.10 The Contractor shall support the training design and development phases (or process) by providing and collaborating with the OCMT team on an ongoing basis in the following ways, including but not limited to:
  - A.20.10.1.1 Aligning project plan(s) and validating major milestones to support training timelines
  - A.20.10.1.2 Providing existing and historical baseline training materials (in digital or print format as required by the State) such as but not limited to train-the-trainer training manuals, quick reference guides, PowerPoints, simulations, etc.
  - A.20.10.1.3 Actively participating and providing information during training development knowledge share sessions

- A.20.10.1.4 Training and supporting the State-appointed OCMT personnel on any and all system specific work areas, processes, applications, etc. as deemed appropriate by the State for the purposes of executing a system-based scenario training program to all impacted State personnel
- A.20.10.1.5 Providing, as requested, validation of future-state process information and documentation
- A.20.10.1.6 Providing or cooperating in the identification of realistic, representative business scenarios to be used for training development and delivery purposes as defined by the State
- A.20.10.1.7 Providing access to the training development environment at the outset of the training development phase
- A.20.10.1.8 Coordinating and supporting the development and maintenance of hardware requirements (for example, but not limited to, classroom computers or laptops, independent servers that might be required to house training development tools and associated content, etc.) with the State for training delivery purposes
- A.20.10.1.9 Providing a minimum of one hundred (100) training laptops and other required physical hardware to support the training design and implementation of all TEDS-related trainings
- A.20.10.1.10 Maintaining training and laptop software, hardware, and system services required by each release's training needs.
  - a) The Contractor shall ensure that each provided laptop has, at a minimum, been configured with, and can successfully run, the then most current version of Microsoft Suite products, Internet Explorer and Adobe Reader.
  - b) The Contractor shall ensure that each laptop system has sufficient access to the then current TEDS training environment(s) and other associated software that will be required for training purposes.
  - c) The Contractor shall determine, with the assistance of the State, the most efficient manner to access these environments through a combination of downloaded and internet accessible applications.
  - d) The Contractor shall ensure that each laptop is installed and maintained with virus protection software that meets the State requirements at time of usage.
  - e) The Contractor shall provide the State any necessary advice and support to ensure that the laptops software is functioning in a consistent and secure manner throughout training preparation and course delivery.
  - f) The Contractor shall maintain the required installed software with the most current software versions and/or patches throughout the timeframe of the engagement.
- A.20.10.1.11 Adhering to the State's approved OCMT QM process

- A.20.11 The Contractor shall support the Training Implementation phase (or process) by providing and collaborating with the OCMT Team on an ongoing basis in the following ways, including but not limited to:
- A.20.11.1 Delivering (or supporting the delivery of) and actively participating in training and/or classroom sessions and activities as needed and defined by the State in order to provide subject matter expertise in specific work areas, processes, applications, etc. (supplying at least one (1) Subject Matter Advisor in each discreet classroom training event)
  - A.20.11.2 Providing feedback on training program for continuous improvement efforts
  - A.20.11.3 Providing necessary support for the appropriate maintenance of the training environment (e.g., making updates to scenarios or transactional data to support continuous improvement)
  - A.20.11.4 Providing necessary resources to execute and maintain an active training environment refresh schedule based on scheduled training events to support any and all potential concurrent classes defined by the training schedule
  - A.20.11.5 Actively participate in any and all necessary hardware and other training infrastructure support activities to ensure smooth and consistent training delivery
  - A.20.11.6 Training Delivery shall begin no fewer than two (2) months prior to each release and remain open for no fewer than one (1) month after each release as required by the State
- A.20.12 The Contractor shall support the Training Evaluation phase or process by providing and collaborating with the OCMT Training team in the following ways, including but not limited to:
- A.20.12.1 Developing a Knowledge Transition Plan that encompasses prior training support activities delivered or supported by the Contractor
  - A.20.12.2 Providing support of Post Go-Live training events that encompasses prior training support activities delivered or supported by the Contractor for a period of time as deemed reasonable by the State
- A.20.13 The Contractor shall support any and all CMS related awareness and training. The Contractor shall work with the OCMT team to ensure that the course is incorporated into the overall curriculum, and the Contractor shall provide all relevant content/SME input, and ensure that the presentation and delivery is consistent with State curriculum standards
- A.20.14 The Contractor shall support any and all other training activities to ensure an effective, positive learning experience as required by the State
- A.20.15 The Contractor shall provide a full-time, dedicated OCMT counterpart with appropriate OCMT background, to be approved by the State, whose responsibilities shall include, at a minimum, the effective and timely execution of any and all OCMT activities throughout the duration of all relevant Program project lifecycles
- A.21 Quality Assurance and Monitoring

- A.21.1 The Contractor shall comply with the State's Quality Assurance Plan. The Contractor shall maintain compliance with all Plan components including project management and staff, contractors, and other participants in the project and all project activities.
- A.21.2 The Contractor shall collaborate with the State to align the Contractor's Quality Assurance Plan to the State's Plan to support the monitoring methodology for the DDI stage of the project.
- A.21.3 The Contractor shall provide an overall Quality Assurance Plan, customized for the EMP.
- A.21.4 The Contractor shall establish QA roles & responsibilities internally and with the State Project Manager and sponsor.
- A.21.5 In conjunction with the State and Other State Contractors, the Contractor shall support the internal QA process, including adhering to quality standards and supporting the effort to validate and verify that standards are met.
- A.21.6 The Contractor shall provide access and training for usage of any tools that will be used in implementing and monitoring the process
- A.21.7 The Contractor shall incorporate a QA review which results in remediation plans for both current and future project deliverables.
- A.21.8 The Contractor shall conduct internal quality reviews for all deliverables before the deliverables are submitted to the State.
- A.21.9 The Contractor shall support QA reviews performed by the State or State Contractors. The activities for which they will support include, but are not limited to: deliverable walkthroughs, incorporating revisions into deliverables, and supporting Gate Reviews.
- A.21.10 The Contractor shall monitor the performance of each service against the service specific KPIs defined in Deliverable 28. The Contractor shall be responsible for reporting the KPIs and the associated supporting metrics at an agreed upon frequency with the State. The Contractor shall also be responsible for maintaining the agreed upon SLAs associated with these KPIs and supporting metrics as designated by the State. The State reserves the right to require the Contractor to monitor and report on additional KPIs for performance areas based on deficiency. The KPI SLA reporting shall be input into the Contractor's CIP, described in detail in Section A.17.2.

## A.22 Staffing

- A.22.1 **General Staffing Requirements.** All personnel shall be employees or contracted staff of the Contractor and shall be fully qualified to perform the work required in this Contract. The Contractor shall provide experienced, qualified professionals to ensure the success of this project. Contractor personnel shall be qualified, allocated, present, focused and engaged with State, other State entities and other State Contractors. The Contractor shall provide these personnel in sufficient quantity to enable the Contractor to provide consistent and high quality deliverables and supporting work product, even during periods in which work on multiple projects are underway.
  - A.22.1.1 Contractor work will normally occur during the State's core business hours (8:00 AM to 5:00 PM Central time, Monday through Friday), during which the Contractor must provide coverage of key business areas. As directed by the State, exceptions may occur to accommodate scheduled project events that must occur during evenings or on weekends. The parties agree that the Contractor will furnish

Contractor personnel as needed for these after-hours projects. Contractor work and travel schedules shall be approved in advance by the Program Director. The Contractor shall have production support staff available twenty four (24) hours per day seven (7) days per week during Operations and Maintenance.

- A.22.1.2 Other than required approval of Key Personnel and subcontracted staff by the State, the Contractor shall have total responsibility for hiring and management of any and all Contractor staff and subcontractors determined necessary to perform the services in accordance with the terms of the Contract. The Contractor is responsible for maintaining a level of staffing necessary to perform and carry out all of the functions, requirements, roles, and duties as contained herein, regardless of the level of staffing included in its proposal. After consultations with the Contractor, the State shall make the final decision as to the required staffing levels based upon current progress in meeting the goals of the EMP and anticipated future needs for the Solution. The State will use the CM process to indicate dates by which staffing increases or replacements must be made. Failure to meet the staffing deadlines in the CM may lead to the imposition of Liquidated Damages as specified in Section A.22.10.4.
- A.22.1.3 On-site Staffing Requirements. For purposes of this Contract, whenever the term "on-site" appears, it shall mean that the indicated Contractor staff and/or subcontractors shall be physically present during the percentages identified in Section A.22.15 and A.22.16, from their start date throughout the term of the Contract or until they are no longer performing services under the Contract. Personnel are considered on-site when working at either the Contractor's offices described in Section A.23 or at the HCFA offices located in Nashville, Tennessee as required by the State. "On-site" positions also require the Contractor staff and/or subcontractors to meet the dedication requirements for each role. Percentage dedicated means that the personnel shall be assigned to work the required portion of their time on the services to be provided under this Contract and the personnel may not work full or part time on other work unless approved in advance in writing by the State.
- A.22.1.3.1 Roles that are established to support Operations and Maintenance through the remainder of the Contract and that are staffed shall be included in the measurement of Operations and Maintenance headcount for a given period, even though they may also be supporting enhancement activity for the same period.
- A.22.1.4 State approval of Contractor's Staff. The State shall have the discretion to approve or disapprove of the Contractor's and any of its subcontractor's staff, or to require the removal or reassignment of any Contractor's employee or subcontractor personnel found unacceptable to the State for work under this Contract only.
- A.22.1.5 Contractor Staff and CMS Reporting Requirements. The Contractor shall keep track of resource costs, both personnel and technical, on a per project basis in order to satisfy both the State and CMS reporting requirements for enhanced federal funding assistance. These resource costs shall be maintained by the Contractor and provided to the State upon request to support all projects. After consultation with the Contractor, the State will approve an invoice format that will meet the needs of the State and CMS. The Contractor shall submit an invoice in the required format for approval once the State has issued its acceptance of the deliverable.

- A.22.2 Subcontracted Staff. The Contractor may not subcontract, transfer, or assign any portion of the Contract without prior written approval of the State given after review and approval of the Contractor's proposed subcontract, transfer agreement, or assignment agreement. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment and to revoke, at any time, its prior written approval of any subcontractor, transferee or assignee.

With regard to those subcontractors approved by the State during procurement of this Contract, the Contractor shall provide the State with a fully executed, complete copy of each subcontract on or before the earlier to occur of: (a) such subcontractors beginning work on this Contract, or, (b) within thirty (30) days of execution of the Contract. With regard to subcontractors approved by the State and engaged by Contractor after the Contract start date, the Contractor shall provide the State with a fully executed, complete copy of each subcontract on or before the earlier to occur of: (a) such subcontractors beginning work on this Contract, or, (b) within thirty (30) days of the State's approval of the subcontract.

The Contractor may only substitute another subcontractor for a subcontractor previously approved by the State at the discretion of the State and with the State's prior, written approval.

Notwithstanding any State approval relating to subcontracts, the Contractor shall be the prime contractor and shall be responsible for all work under the Contract.

- A.22.3 Key Personnel Requirements. For purposes of this Contract, the term "Key Personnel" refers to Contractor personnel deemed by the State to be essential to the Contractor's satisfactory performance of the requirements contained in this Contract. Contract Section A.22.15 contains the required Key Project Personnel positions, corresponding roles and responsibilities and minimum qualifications for each.

- A.22.3.1 All Key Personnel shall be employed by the Contractor and be present full-time at either the Contractor's offices described in Section A.23 below or at HCFA's offices in Nashville, Tennessee from their start date throughout the project. Changes to this arrangement must receive prior approval from the State.
- A.22.3.2 The Contractor shall obtain written prior State approval of all Key Personnel. Resumes for Key Personnel must be provided for State review at least thirty (30) days prior to the expected employee's start date. The State may require in-person interviews with these individuals prior to the employee's start date. The same person may be able to fill a different position in different Gate Reviews. The State will consider suggestions for alternative alignment of duties. Changes to the proposed positions, staff and responsibilities will only be allowed with prior written permission from the State.
- A.22.3.3 If the Contractor's methodology deems an additional Key Personnel position(s) necessary, beyond the positions listed in the table below, the Contractor must identify these positions and provide a complete description of how these positions support the fulfillment of the Contract scope of work. All Contractor Key Personnel must be formally committed to join the project by the beginning of the Contract start date.
- A.22.3.4 If any Contractor staff members are not employees of the Contractor, the Contractor is required to identify those personnel, provide the State with agreements establishing their subcontract and the Contractor must receive approval of that subcontract with the State.

- A.22.3.5 References for Key Personnel shall meet the following requirements:
- A.22.3.5.1 Must include a minimum of three (3) professional references outside the employee's current employer who can provide information about the key person's work on relevant past assignments;
  - A.22.3.5.2 Must include the reference's full name, mailing address, telephone number and e-mail address;
  - A.22.3.5.3 For any client contact listed as a reference, must also include the agency's or company's full name with the current telephone number and e-mail address of the client's responsible project administrator or service official who is directly familiar with the key person's performance;
  - A.22.3.5.4 Must reflect the key person's professional experience within the past five (5) years; and
  - A.22.3.5.5 Must include all professional certifications and affiliations.
- A.22.3.6 Key Personnel resumes shall include the following information:
- A.22.3.6.1 Employment history for all relevant and related experience
  - A.22.3.6.2 Names of employers for the past five (5) years, including specific dates
  - A.22.3.6.3 All education institutions attended and degrees obtained
- A.22.4 Key Personnel Replacements. The State retains the right to approve or disapprove proposed Key Personnel staffing and reserves the right to require the Contractor to replace specified staff. The Contractor agrees to substitute, with the State's prior approval, any employee so replaced with an employee of equal or better qualifications. The Contractor shall provide an interim resource within five (5) business days for any Key Personnel vacancies regardless of the reason for the vacancy. The Contractor agrees to propose within thirty (30) days, and appropriately staff within forty-five (45) days, any changes made to Key Project Personnel, regardless of the reason for the change. In the event it becomes necessary to replace Key Personnel during the term of this Contract, the Contractor shall:
- A.22.4.1 Provide the State Program Director with written notification of such replacement, providing, when possible, for a two (2) week period for knowledge transfer from the Key Personnel to the replacement personnel. This knowledge transfer shall be provided at no charge to the State;
  - A.22.4.2 Provide the State Program Director with documentation describing the circumstances of the need for the replacement;
  - A.22.4.3 Provide documentation of experience for the proposed replacement personnel; and
  - A.22.4.4 Obtain prior written approval from the State Program Director.
  - A.22.4.5 During the first eighteen (18) months of the Contract performance period, no substitutions of Key Personnel shall be permitted unless such substitutions are necessitated by an individual's sudden illness, death, or resignation, or otherwise approved by the State Program Director or requested by the State. In any of these

events, the Contractor shall follow the steps outlined above. Failure to meet the prior notice and approval requirements herein may result in the imposition of Liquidated Damages as contained in Section A.22.10.4.

- A.22.5 Non Key Personnel Requirements. The Contractor shall ensure that a State-approved number of appropriately qualified and trained personnel are employed and available at all times to provide the services required under the Contract. Staff proposed for assignments shall be persons that have relevant domain knowledge as appropriate for such job title classifications.

Unless otherwise agreed by the State, the job title classification of individuals assigned to a project shall not change during the project.

In providing the services required under this Contract the Contractor shall provide, at a minimum the Non-Key Personnel identified in Section A.22.16. The quantity of the personnel for each of the positions shall be State-approved and shall provide an appropriate level of service for the TEDS.

A.22.6 Staffing Management Plan

- A.22.7 The Contractor shall develop and adhere to a Staffing Management Plan for conducting the day-to-day management of all resources in support of EMP activities. The Plan shall define the organizational structure, roles, and responsibilities of the personnel, staffing levels, and other resources information. It shall define the criteria and process used to develop staffing estimates and determine staffing qualifications. It shall contain detailed organizational charts. The organization structure must identify Key Personnel by name, title and job function, the percentage of time allocated to the EMP, and whether each position will be filled by a State person, Contractor employee, or other Contractor employees (i.e. TAS or SPMO).

A.22.8 Staffing Needs Planning and Monitoring Processes

- A.22.8.1 The Contractor shall provide an overview of the preliminary and ongoing Staff Planning and Monitoring Processes, specifically highlighting processes around planning for future needs and monitoring of project assignments, contract timelines, and associated decisions for release or renewal of personnel.

A.22.9 Staffing Tracker

- A.22.9.1 The Contractor shall develop a Staffing Tracker that summarizes initial and ongoing Solution resource needs and documents resource levels and assignments.
- A.22.9.2 The Contractor shall maintain and update the Staffing Tracker on a regular basis for review, at least once per quarter and more frequently as requested by the State.

A.22.10 Key Personnel Transitions

- A.22.10.1 The Contractor shall develop a Key Personnel Transition Plan, for completion by Key Personnel in the event that they change roles or leave the project. Completed Plans shall identify a replacement for the Key Personnel in question.
- A.22.10.2 The Contractor shall seek prior approval from the State for any replacements to be made in key roles. The Contractor may replace Key Personnel with individuals

with comparable experience and qualifications as those submitted by the Contractor in their Response to RFQ 32101-15557 within fifteen (15) business days, pending State approval. The Contractor shall submit resumes and allow the State to interview applicants as part of the approval process, at least five (5) business days before the intended start date.

- A.22.10.3 The Contractor shall provide an interim resource within five (5) business days for any Key Personnel vacancies regardless of the reason for the vacancy.
- A.22.10.4 Staffing Liquidated Damages. Failure by the Contractor to meet the timeframes for staffing vacancies and replacements as set forth in Sections A.22.4 and A.22.3, or any staffing timeframe contained in a CM as specified in A.22.1.2, may, at the State's sole discretion, result in Liquidated Damages in the amount of five hundred dollars (\$500) per business day until Contractor complies with the stated timeframe.
- A.22.10.5 The Contractor shall maintain a State-approved quantity of staff composed of Project Managers, Business Analyst, Programmer Analyst, and Testers to accommodate enhancements during Operations and Maintenance (O&M).
- A.22.11 Managing Staffing Changes
- A.22.11.1 The Contractor shall provide an overview of the key steps required in order to acquire, onboard, and off-board staff.
- A.22.11.2 The Contractor shall provide guidance on the necessary steps to make staffing assignment changes. The Contractor shall also define procedures for Key Personnel transitions.
- A.22.11.3 The Contractor shall develop the following documents for managing staffing changes and use the documents in the processes as detailed in the table below:

*Table 2: Documents*

Form	Onboarding	Role Transitions	Off-Boarding
Onboarding Checklist	X		
Onboarding Arrival Packet	X		
Acceptable Use Policy and Information Protection Plan	X		
Roll-On Form	X	X	
Team Member Transition Plan		X	
Roll-Off Form			X
Off-Boarding Checklist			X

- A.22.11.4 The Contractor shall develop an Onboarding Checklist to assist in onboarding new resources. The Onboarding Checklist shall provide the new employee with an orientation to the EMP and relevant State and Federal regulations and policies. Additionally, the Checklist shall ensure that administrative items such as building access and equipment distribution are appropriately handled.
- A.22.11.5 The Contractor shall develop a Team Member Transition Plan to be completed by Contractor resources when assignments change within the project organization.
- A.22.11.6 The Contractor shall submit all completed plans to the SPMO for review and validation.

A.22.11.7 The Contractor shall provide at least two (2) weeks' notice before resource roll-off.

#### A.22.12 Turnover Stage Staffing

A.22.12.1 The Contractor shall provide a full-time turnover manager as a designated point person to interact with the State and successor contractor until Contract closeout is completed.

A.22.12.2 The Contractor shall provide and retain sufficient turnover staff in the required mix, inclusive of technical (e.g. systems analysts, technicians) and non-technical (e.g. clerical staff, business analysts) resources to complete the services and meet the requirements specified in the Contract.

A.22.12.3 The Contractor shall include in the Staffing Management Plan staffing for operations during the Turnover Stage.

A.22.12.4 The Contractor shall acquire State approval for Key Personnel appointments and replacements.

A.22.12.5 The Contractor shall provide unrestricted access to appropriate Contractor personnel for discussion of problems or concerns.

A.22.12.6 The Contractor shall provide, at minimum, a two (2) week overlap transition period for all Key Personnel transitions. During this time the successor shall be trained on all transferred activities to ensure continuity.

#### A.22.13 Off-Boarding

A.22.13.1 The Contractor shall complete the Off-Boarding Checklist, one (1) week prior to resource departure, with assistance from the work stream lead and the team member rolling off.

A.22.13.2 The Contractor shall provide prior notification, in the event of resource departure, with appropriate forms to the State's Access Management team and appropriate State management staff, in advance of termination if known or immediately after the employee submits their resignation.

#### A.22.14 CMS Certification

A.22.14.1 The Contractor shall provide a State-approved quantity of staff to support the enhanced efforts to monitor, identify, and address initial production issues and plan, prepare, execute, and achieve CMS certification.

A.22.14.2 The Contractor shall provide a Certification Manager to interact in tandem with the State and the IV&V Contractor.

A.22.14.3 The Contractor shall provide a State-approved team of resources to monitor, track, and correct identified issues.

A.22.14.4 The Contractor shall provide an State-approved team of dedicated resources for preparation and support of CMS certification.

## A.22.15 Key Personnel Table

Table 3: Key Personnel Table

Key Position	Description	Qualifications	Requirements
<b>Account Executive or Program Executive</b>	a) Shall serve as the onsite program executive for the Contractor	<ul style="list-style-type: none"> <li>a) A minimum of eight (8) years of experience in managing and leading a large-scale or enterprise-wide health care IT systems contract or project that encompasses a full SDLC from initiation through post implementation and includes Operations and Maintenance.</li> <li>b) A minimum of five (5) years of experience serving in an account management or client representative position.</li> <li>c) Subject matter expertise on State and Federal Medicaid regulations and policies.</li> <li>d) Previous experience with cost reporting, profit and loss statements, and budget compliance.</li> <li>e) Previous responsibility for managing subcontractor resources, if subcontractors are included as part of the Contractor's Response to RFQ 32101-15557.</li> <li>f) Previous experience following a standard project management methodology and in using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources.</li> <li>g) Broad IT-related experience</li> <li>h) PMI or generally equivalent certification.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>DDI Manager</b>	a) Responsible for the Design, Development, and Implementation of eligibility Solution	<ul style="list-style-type: none"> <li>a) A minimum of ten (10) years of experience implementing and integrating large-scale health care IT solutions within environments similar to that of the TEDS.</li> <li>b) Subject matter expertise on State and Federal Medicaid regulations and policies.</li> <li>c) Previous experience following the Contractor's development methodology and in using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

Key Position	Description	Qualifications	Requirements
		<ul style="list-style-type: none"> <li>d) Heavy background in IT development, infrastructure, security, and Operations and Maintenance projects.</li> <li>e) Relevant experience and advanced skills with development tools, multiple software languages, and programming best practices.</li> <li>f) PMI certification is preferred.</li> </ul>	
<b>Technical Solution Lead</b>	<ul style="list-style-type: none"> <li>a) Shall serve as the project Chief Information Officer (CIO) for the eligibility Solution.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of seven (7) years of experience implementing large-scale health care IT solutions within environments similar to that of the TEDS.</li> <li>b) Possess expert knowledge of the Contractor's Solution, having implemented the Solution in no less than one (1) environment at least as complex as the TEDS.</li> <li>c) Possess extensive experience developing solutions utilizing an integrated development environment, multi-tier platforms and employing SOA architecture with high availability/reliability requirements.</li> <li>d) Must be proficient in multiple languages, SOA technologies, operating systems and security best practices.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Business Solution Lead</b>	<ul style="list-style-type: none"> <li>a) Shall serve as the project Chief Operations Officer for the eligibility Solution.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of seven (7) years of experience implementing large-scale health care IT solutions within environments similar to that of the TEDS</li> <li>b) Possess five (5) years of experience extracting and documenting business rules</li> <li>c) Possess a working knowledge of business process modeling</li> <li>d) Possess expert knowledge of the Contractor's Solution, having implemented the Solution in no less than one (1) environment at least as complex as the TEDS</li> <li>e) Possess expert knowledge of national policy and standards that impact the Medicaid environment.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Quality</b>	<ul style="list-style-type: none"> <li>a) Shall serve as the project QA</li> </ul>	<ul style="list-style-type: none"> <li>a) Possess a minimum of five (5) years of</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other</li> </ul>

Key Position	Description	Qualifications	Requirements
<b>Assurance/Control Lead</b>	<p>Manager for the eligibility Solution</p> <p>b) Responsible for EMP quality control</p>	<p>experience developing and executing quality assurance/control programs for solutions similar to the Contractor's Solution for the TEDS</p> <p>b) Previous experience serving in a Quality Control Manager or Lead position.</p> <p>c) Possess a working knowledge of the Contractor's Solution for the TEDS.</p> <p>d) Previous experience leading large scale or enterprise-wide testing rollouts and deployments.</p> <p>e) Possess a working knowledge of business processes associated with the TEDS.</p> <p>f) Must have general knowledge with multiple programming languages, SOA technologies, operating systems and security best practices.</p>	<p>position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</p> <p>c) Shall be onsite ninety percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<b>OCMT Liaison</b>	<p>a) Working closely with State designated team to make sure deliverables are met on time and on budget</p> <p>b) Coordinate and Manage instructional design staff</p> <p>c) Liaison between parties to address obstacles and ensure time access to all required systems</p> <p>d) Adherence to project plan</p> <p>e) Working with State Project OCMT Team to support the development of relevant materials and timely deliverable of all training requests</p> <p>f) Facilitate working relationship with State OCMT Team and SME's</p> <p>g) Facilitate working sessions between State OCMT Team and SME's to conduct knowledge sharing sessions</p> <p>h) Facilitate working sessions between State OCMT Team and</p>	<p>a) Possess a minimum of five (5) years of experience developing and executing training programs for solutions similar to Contractor's Solution for the TEDS.</p> <p>b) Possess a working knowledge of document management practices and principles.</p> <p>c) Possess a working knowledge of the Contractor's Solution for the TEDS.</p> <p>d) Possess a working knowledge of business processes associated with the TEDS.</p> <p>e) Previous experience working with document management platforms to include document version control and management workflow</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be on-site for all training activities.</p>

Key Position	Description	Qualifications	Requirements
	SI's technical groups for collaboration and knowledge sharing		
<b>Project Management Office (PMO) Manager</b>	<ul style="list-style-type: none"> <li>a) Shall serve as the Contractor liaison to the SPMO and TAS Contractors.</li> <li>b) Responsible for project's PMO.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years of experience developing and managing a PMO for a large scale or enterprise-wide health care IT systems contract or implementation.</li> <li>b) A minimum of ten (10) years of experience managing IT systems programs and/or projects.</li> <li>c) Must be PMI certified.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be allocated one hundred percent (100%) to the project through implementation.</li> </ul>
<b>Infrastructure Architect</b>	<ul style="list-style-type: none"> <li>a) Responsible for defining and documenting network, security, server, SOA and the OS specifications for the Solution.</li> <li>b) Shall ensure that policies, standards, and procedures related to infrastructure are established, communicated, and enforced</li> <li>c) Shall work closely with the HCFA IS Architect and STS to translate the infrastructure architecture for the Solution into build standard STS build specifications.</li> </ul>	<ul style="list-style-type: none"> <li>a) Possess a minimum of five (5) years of IT infrastructure management experience with a strong preference towards healthcare environments.</li> <li>b) Possess a minimum of three (3) years of experience managing projects of similar size and complexity.</li> <li>c) Must have advanced knowledge working with multiple programming languages, SOA technologies, operating systems and security best practices.</li> <li>d) Expert understanding of OS(s) that Solution is running on</li> <li>e) Strong understanding of VMWare</li> <li>f) Solid understanding of Load Balancing (F5 LTM &amp; GTM preferred)</li> <li>g) Solid understanding of Internet access using a DMZ for things such as, but not limited to: proxies, web servers, firewalls, DNS and Certificates</li> <li>h) Knowledge of complex network routing</li> <li>i) Familiarity of DBMS used for Solution</li> <li>j) Solid knowledge regarding Storage Area Networks (Preferably Hitachi).</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not service in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be allocated 75% through subsequent deployments of DDI.</li> <li>e) Shall be available as needed post Go-Live.</li> </ul>
<b>Configuration &amp; Assets Manager</b>	<ul style="list-style-type: none"> <li>a) Service Assets Management</li> <li>b) Configuration Items Management</li> <li>c) Product Currency Management</li> <li>d) License Management</li> <li>e) CMDB Implementation &amp;</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience in a configuration and assets manager role for a large scale, mission critical environment</li> <li>b) Possess knowledge of working with multiple programming languages, SOA technologies,</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>b) Shall be onsite ninety percent (90%) percent of the</li> </ul>

Key Position	Description	Qualifications	Requirements
	Management	operating systems and security best practices c) Possess ITIL certification	time
<b>Service Desk, Production Control &amp; Operations Center Manager</b>	<ul style="list-style-type: none"> <li>a) Shall serve as the project Operations Manager for the eligibility Solution</li> <li>b) Shall have the responsibility for monitoring and support of the Solution.</li> <li>c) Shall prepare the daily/monthly Operations Report.</li> <li>d) Manage staff 7/24/365 and ensure reliability and availability for multiple system platforms including infrastructure, databases, backups, trouble shooting, problem resolution, escalation, and notification.</li> <li>e) Schedule and coordinate batch jobs, system installs, upgrades and outages.</li> <li>f) Establish priority problem resolution, notification and escalation to appropriate support personnel to meet schedules and Service Level Agreements</li> <li>g) Monitor and administer support and services for all Production Control, Service desk, and operations activities including perform all batch scheduling, production activities, printing, and print distribution.</li> <li>h) Provide application, hardware, network, schedule support and system monitoring for the Solution.</li> <li>i) Shall be responsible for the development and maintenance of the SOP manual.</li> </ul>	<ul style="list-style-type: none"> <li>a) Possess a minimum of five (5) years' experience managing Production Control/Operations management of a 24/7/365 environment on large-scale health care programs and solutions similar to the environments and scale of the TEDS.</li> <li>b) Possess (5) years' experience in managing networks, servers, batch scheduling, console activities, service desk management, and security similar to the technical architecture for the TEDS.</li> <li>c) Must have advanced knowledge working with output management, print, console operations, system administration, operating systems, production control scheduling, technical writing, and security best practices</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be allocated one hundred percent (100%) to the project beginning from UAT through ongoing operations</li> <li>b) Shall be on site one hundred percent (100%) of the time</li> </ul>
<b>Security</b>	a) Responsible for managing the	a) Possess a minimum of five (5) years IT	a) Shall not serve in any other

Key Position	Description	Qualifications	Requirements
<b>Manager</b>	<p>implementation and development of IT security over the course of the project.</p> <ul style="list-style-type: none"> <li>b) Shall ensure that security policies, standards, and procedures are established and enforced.</li> <li>c) Shall coordinate information security inspections, tests, and reviews and oversee the security team.</li> <li>d) Responsible for coordination and compliance activities relative to the project including, but not limited to, MARS-E, Fortify reporting, audit, SSR, etc.</li> </ul>	<p>security industry experience with at least three (3) years in a healthcare related environment.</p> <ul style="list-style-type: none"> <li>b) Possess a minimum of three (3) years of experience managing projects of similar size and complexity to the EMP.</li> <li>c) Possess a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or equivalent security certification (e.g., GIAC (Global Information Assurance Certification) Security Expert, Certified Ethical Hacker, GIAC Certified Incident Hacker, GIAC Web Application Penetration Tester, GIAC Penetration Tester)</li> <li>d) Possess a Bachelor's Degree in an IT-related field OR four (4) years of industry experience in addition to the general requirement for five (5) years of security experience.</li> <li>e) Must be familiar with at least one major security compliance framework and be able to demonstrate a firm understanding of relevant State and Federal security/privacy regulations and policies, specifically under NIST, HIPAA, and IRS Pub. 1075</li> <li>f) Must have excellent communications skills, technical writing skills, small group facilitation skills, and formal presentation skills.</li> </ul>	<p>position.</p> <ul style="list-style-type: none"> <li>b) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> </ul>
<b>CIP Manager</b>	<ul style="list-style-type: none"> <li>a) Shall collect data, compile, and report on KPIs and SLAs.</li> <li>b) Responsible for managing the customer expectations and all CIP functions.</li> <li>c) Gather and analyze metrics to accurately reflect schedule performance relative to established SLAs.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of eight (8) years of experience in managing large scale or enterprise-wide technology projects. Must have broad experience managing IT systems contracts, SLAs, KPIs, and process improvement programs.</li> <li>b) Must have working experience with system design and capacity planning.</li> <li>c) A minimum of five (5) years of experience serving in an IT management position in a technical area.</li> <li>d) Subject matter expertise on system design, system build, and O&amp;M.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

Key Position	Description	Qualifications	Requirements
		<ul style="list-style-type: none"> <li>e) Previous experience with ITIL and other operating frameworks.</li> <li>f) Must have relevant IT experience with all technical aspects of the Solution.</li> </ul>	
<b>Database Architect</b>	<ul style="list-style-type: none"> <li>a) Responsible for designing, developing, and implementing infrastructure to provide highly-complex, reliable, and scalable databases to meet the organization's objectives and requirements.</li> <li>b) Shall assist in defining system and application architecture and provide vision, problem anticipation, and problem solving ability.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience developing and implementing one or more industry standard database systems.</li> <li>b) Capable of hands-on work in all phases of database design and management</li> <li>c) Significant experience managing operational databases including handling complex migrations with mission critical applications</li> <li>d) Extensive experience dealing with sensitive data, and health care industry standards and regulations</li> <li>e) Experience with technical requirements for data classification and implementing data protection technologies.</li> <li>f) Must be knowledgeable of secure coding practices for databases.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Conversion Manager</b>	<ul style="list-style-type: none"> <li>e) Oversees the conversion of legacy data into the EMS database.</li> <li>f) Coordinates and manages Conversion staff and tasks.</li> <li>g) Works with all appropriate staff to coordinate conversion efforts.</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience managing complex conversion projects from disparate legacy databases into different data models.</li> <li>b) Must have experience with the Contractor's chosen ETL/Conversion toolset (at least two (2) prior conversions).</li> <li>c) Experience with managing and documenting conversion efforts and staff.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> <li>d) Shall be available as needed post Go-Live</li> </ul>
<b>Application Architect</b>	<ul style="list-style-type: none"> <li>a) Shall provide application architecture and design recommendations based on existing State standards.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years of experience building and supporting mission critical, multi-tier large scale health care applications.</li> <li>b) Shall be knowledgeable of secure coding practices.</li> <li>c) Experience with technical requirements for data classifications and implementing data protection technologies.</li> <li>d) Must possess extensive experience</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> </ul>

Key Position	Description	Qualifications	Requirements
		<ul style="list-style-type: none"> <li>developing solutions utilizing an integrated development environment, multi-tier platforms and employing SOA architecture with high availability/reliability requirements.</li> <li>e) Must be proficient in multiple languages, SOA technologies, operating systems and security best practices.</li> </ul>	<ul style="list-style-type: none"> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>SOA Architect</b>	<ul style="list-style-type: none"> <li>a) Shall design and implement the integration between the TEDS and other State standard COTS software</li> <li>b) Shall use the latest SOA technologies and Web Services frameworks</li> </ul>	<ul style="list-style-type: none"> <li>a) Experience with Oracle Service Bus and Business Process Execution Language service development – Web Services, SOAP, Web Service Description Language, XML, Extensible Stylesheet Language Transformations, XML Path Language, Hyper Text Markup Language, and Universal Description, Discovery, and Integration</li> <li>b) Knowledge includes advanced work on standard applications programs including coding, testing, and debugging</li> <li>c) Strong knowledge of the object-oriented analysis and design patterns/techniques</li> <li>d) Extensive experience with web applications.</li> <li>e) Must possess extensive experience developing solutions utilizing an integrated development environment, multi-tier platforms and employing SOA architecture with high availability/reliability requirements.</li> <li>f) Must be proficient in multiple languages, SOA technologies, operating systems and security best practices.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

## A.22.16 Non-Key Personnel Table

Position	Description	Qualifications	Requirements
<b>Technical Solution Architect</b>	<ul style="list-style-type: none"> <li>a) Enterprise Architecture</li> <li>b) Build book planning and design</li> <li>c) Demand Management</li> <li>d) Availability Planning</li> <li>e) Capacity Planning</li> <li>f) Security &amp; Privacy compliance</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience implementing large-scale health care IT solutions within environments similar to that of the TEDS</li> <li>b) Experience implementing data warehouse solutions within an integrated environment and employing SOA and intelligent business reporting.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> </ul>

Position	Description	Qualifications	Requirements
		<ul style="list-style-type: none"> <li>c) Must possess extensive experience developing solutions utilizing an integrated development environment, multi-tier platforms and employing SOA architecture with high availability/reliability requirements.</li> <li>d) Must be proficient in multiple languages, SOA technologies, operating systems and security best practices.</li> </ul>	<ul style="list-style-type: none"> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Technical Specialist Application and Web Platforms</b>	<ul style="list-style-type: none"> <li>a) Platform support including troubleshooting, contributing to root cause analysis, and problem resolution</li> <li>b) Identifying and assessing risks, determining impact to platform and mitigation plans</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience with Web technologies and tools</li> <li>b) Strong Systems Administration skills</li> <li>c) Web hosting, caching and proxy software and related technologies</li> <li>d) Extensive knowledge of Web Application and Operating System security</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be allocated one hundred percent (100%) to the project through Implementation.</li> <li>c) Shall be on site ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Database Administrator</b>	<ul style="list-style-type: none"> <li>a) Shall recommend solutions by defining database physical structure and functional capabilities, database security, data back-up, and recovery specifications.</li> <li>b) Shall maintain database performance by calculating optimum values for database parameters, implementing new releases, completing maintenance requirements, and evaluating computer operating systems and hardware products.</li> <li>c) Responsible for maintaining separation of duties as required by security industry standards.</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience managing a complex RDBMS environment on a UNIX platform with multiple environments (development, test, production, etc.)</li> <li>b) Broad knowledge of database administration tool sets.</li> <li>c) Experience with database software installation, upgrades, management, troubleshooting, design, support (including backups and recovery), data migration techniques and database security</li> <li>d) Extensive experience using and tuning SQL</li> <li>e) Experience with database conversions from disparate systems(s).</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>b) Shall be onsite one hundred percent (100%) of the time.</li> </ul>
<b>Conversion Architect/Programmer</b>	<ul style="list-style-type: none"> <li>a) Designs, programs, tests, and tunes the conversion code to move data from multiple database environments into the Contractor Solution.</li> <li>b) Ensures converted data maintains</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience designing, programming, administering and tuning complex conversions that move data from multiple disparate legacy databases into separate/different data models</li> <li>b) Must have hands on experience with the</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> </ul>

Position	Description	Qualifications	Requirements
	integrity, accuracy and meets performance expectations.	<p>Contractor's chosen ETL/Conversion toolset (at least two (2) prior conversions)</p> <p>c) Experience with writing, testing, configuring and tuning conversion code</p>	<p>c) Shall be onsite ninety percent (90%) percent of the time.</p> <p>d) Shall be available as needed post Go-Live</p>
<b>Interface Lead</b>	a) Shall serve as the project Interface lead for the eligibility Solution	<p>a) Possess a minimum of five (5) years of experience developing and deploying interfaces for systems similar to Contractor's Solution</p> <p>b) Possess a minimum of five (5) years of experience performing data warehouse, data cleansing, or data conversion activities for systems similar to the Contractor's Solution.</p> <p>c) Possess extensive experience supporting multi-tier platforms that employ SOA.</p> <p>d) Shall be familiar with multiple languages, SOA technologies, operating systems, and security industry standards.</p> <p>e) Possess a minimum of three (3) years of experience managing a data conversion or interface design project similar to the needs of the TEDS.</p> <p>f) Possess excellent written and oral communications skills.</p> <p>g) A Bachelor's Degree in IT or a related field is preferred but not required.</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</p> <p>c) Shall be onsite ninety percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<b>Web Portal Specialists</b>	<p>a) Web portal systems administrator</p> <p>b) Proactively monitor and maintain Web Portal environments ensuring high performance, security, and quick issue resolution</p>	<p>a) Minimum of five (5) years of experience administrating web portal services in a large-scale IT environment</p> <p>b) Extensive experience with industry standard web tools</p> <p>c) Strong analytical and problem solving skills</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be allocated one hundred percent (100%) to the project through Implementation.</p> <p>c) Shall be on site ninety percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<b>Senior (Web) Programmer Analyst</b>	a) Assist staff with the analysis of functional business applications, design specifications, and application development.	<p>a) Minimum of eight (8) years' of working experience as a computer specialist or a computer systems analyst</p> <p>b) At least five (5) years' of experience as a</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be allocated one hundred percent (100%) to</p>

Position	Description	Qualifications	Requirements
	<ul style="list-style-type: none"> <li>b) Translates detailed designs into computer software</li> <li>c) Tests, debugs, and refines the computer software to produce the required product</li> </ul>	<ul style="list-style-type: none"> <li>c) Minimum of five (5) years' experience implementing and maintaining web portals</li> <li>d) Web application development using industry standard tools</li> </ul>	<ul style="list-style-type: none"> <li>c) Shall be on site ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Performance Analyst/Capacity Planning Analyst</b>	<ul style="list-style-type: none"> <li>a) Shall develop performance test strategies/methodologies, scripting, and effective execution of the performance strategy.</li> <li>b) Shall perform troubleshooting and analysis to ensure business requirements are met.</li> <li>c) Shall manage, control, and predict the performance, utilization, and capacity of all LAN/WAN network resources and individual network, application, and system components to ensure service level targets are met.</li> <li>d) Shall be responsible for assisting with the development and maintenance of the SOP manual.</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of three (3) years' experience with performance testing and engineering</li> <li>b) Expert understanding of how application usage patterns and behaviors impact and drive needs for capacity resources</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>a) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>b) Shall be onsite ninety percent (90%) of the time.</li> <li>c) Shall be available as needed post Go-Live.</li> </ul>
<b>Programmer Analyst</b>	<ul style="list-style-type: none"> <li>a) Shall develop complex code and scripts for the eligibility Solutions</li> <li>b) Shall assist with design, testing, implementation, and troubleshooting code and scripts throughout the project</li> <li>c) Shall maintain a high level of technical competence in healthcare</li> <li>d) Shall rely on experience and judgment to plan and accomplish goals while balancing priorities.</li> <li>e) Shall function autonomously for most daily work efforts</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience as a Programmer Analyst in a healthcare related industry</li> <li>b) Possess advanced developmental and problem solving skills to support complex application systems and interfaces for large scale healthcare projects.</li> <li>c) Working technical knowledge of platforms and programming languages, including .Net, Visual Basic, C#, JavaScript, Windows Presentation Foundation, and Silverlight.</li> <li>d) Excellent understanding of coding methods and best practices.</li> <li>e) Extensive database experience with Microsoft SQL Server and Oracle.</li> <li>f) Knowledge of applicable data privacy practices and laws</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

Position	Description	Qualifications	Requirements
		g) Hands-on experience developing test cases and test plans	
<b>Senior Business Analyst</b>	<ul style="list-style-type: none"> <li>a) Shall author and present business requirements artifacts that inform the SDLC using Enterprise-standard templates and methodologies (RSA)</li> <li>b) Shall analyze, review, forecast, and trend complex data when necessary</li> <li>c) Shall support short and long term operational/strategic business and IT solutions through research and analysis of data and business processes</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience with a proven record of in-depth knowledge of end-to-end Medicaid eligibility processes</li> <li>b) Able to quickly adjust style and approach to requirements elicitation and communications based on intended audience.</li> <li>c) Experience with the development process for large-scale enterprise applications.</li> <li>d) Experience with general security awareness and processes.</li> <li>e) Possess general IT knowledge.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Business Analyst</b>	<ul style="list-style-type: none"> <li>a) Shall interface with multiple departments within the State and the Contractor to create and/or translate business requirements into technical specifications, deliver quality services using best practices, resolve issues, and track, report, and analyze delivery and process metrics.</li> <li>b) Support, develop, and organize delivery elements, via requirements documentation, process flows, and user stories.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of three (3) years of experience implementing large scale health care IT solutions within environments similar to that of the TEDS.</li> <li>b) Possess expert knowledge of the Contractor's Solution, having implemented the Solution in no less than one (1) environment at least as complex as the TEDS.</li> <li>c) Possess expert knowledge of State and Federal regulations and policies that impact the Medicaid environment.</li> <li>d) Experience with general security awareness and processes.</li> <li>e) Possess general IT knowledge.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) percent of the time</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Process Analyst</b>	<ul style="list-style-type: none"> <li>a) Responsible for end-to-end process activities throughout the project</li> <li>b) Shall create, control, and improve business processes</li> <li>c) Shall lead process design and project implementation teams</li> <li>d) Shall diagnose process improvement opportunities and develop solutions using a data driven approach</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of three (3) years' experience in business process management methodology and concepts</li> <li>b) Understanding of operations in healthcare</li> <li>c) Strong technical, analytical, and problem solving skills</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

Position	Description	Qualifications	Requirements
<b>Quality Assurance Test Manager</b>	<p>e) Shall design and create dashboards, reports, and presentations</p> <p>a) Shall oversee compliance for all of the QA testing processes and procedures, for both functional and non-functional requirements</p> <p>b) Shall create and manage the overall strategic direction of the QA testing team and its testing methodologies</p> <p>c) Responsible for the QA testing team's adherence to processes and procedures, as well as any and all Federal (CMS) and State regulations and policies</p> <p>d) Shall oversee all QA testing phases ( functional and non-functional) and monitor and confirm accurate execution</p> <p>e) Shall create metric reports and status reports</p> <p>f) Shall represent the QA testing team in executive leadership meetings</p> <p>g) Responsible for the staffing of the QA team</p> <p>h) Responsible for writing and deliver of UAT test scripts to the State Test Team Manager</p> <p>i) Shall be responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>a) A minimum of five (5) years' experience in test strategy development, requirements traceability and design specifications, test planning, test case design, integration testing, manual and automated testing, development of defect tracking workflow methodology</p> <p>b) Experience in development of test estimation and staffing requirements.</p> <p>c) Possess extensive experience developing testing solutions in a multi-tier platform SOA environment with high availability/reliability requirements.</p> <p>d) Must be proficient in functional and non-functional test management.</p> <p>e) Experience in managing QA testing staff of ten (10) or more employees.</p> <p>f) Experience in software testing within an agile development methodology</p>	<p>a) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</p> <p>b) Shall be onsite ninety percent (90%) of the time</p>
<b>QA Analyst 3 – Leads</b>	<p>a) Shall receive strategic and tactical guidance from the Test Manager</p> <p>b) Shall implement strategic planning while overseeing daily tactical QA execution</p> <p>c) Shall review and approve requirements.</p> <p>d) Shall create formal test plan</p>	<p>a) A minimum of three (3) years' experience in Quality Assurance, preferably in Health Care or with Medicaid Eligibility Determination</p> <p>b) Capability to implement strategic planning while overseeing daily tactical QA execution</p> <p>c) Experience in requirement review and approval, as well as in testable model analysis</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</p> <p>c) Shall be onsite ninety percent (90%) of the time</p>

Position	Description	Qualifications	Requirements
	<p>documentation based upon requirements and technical design specifications</p> <p>e) Shall confirm technical design specifications' traceability to business requirements.</p> <p>f) Shall serve as liaison to Business Analyst for the QA test team.</p> <p>g) Shall perform sample reviews of test cases and periodically review results of test case execution for accuracy and adherence to policy and procedures.</p> <p>h) Monitor and review all performance test results.</p> <p>i) Shall be responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>d) Experience in review and approval of high-level test scenarios</p> <p>e) Experience in interpretation of requirement and technical design specifications to create formal test plans.</p> <p>f) Capability to interpret technical design specifications in order to clearly communicate with development staff.</p>	<p>d) Shall be available as needed post Go-Live.</p>
<b>QA Analyst 2</b>	<p>a) Shall create test cases based on requirements and assure requirements traceability to test cases.</p> <p>b) Shall peer review test cases.</p> <p>c) Shall perform sample reviews of test cases and periodically review results of test case execution for accuracy and adherence to policy and procedures.</p> <p>d) Shall assure the capture and retention of testing artifacts for audit purposes.</p> <p>e) Shall create test cases and perform performance testing.</p> <p>f) Shall create and execute automated tests.</p> <p>g) Shall be responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>a) A minimum of three (3) years' experience creating and executing test cases based on requirements.</p> <p>b) A minimum of two (2) years' experience of performance and automation testing.</p> <p>c) Experience with peer reviewing test cases</p> <p>d) Capability to review test case expected results for accuracy in adherence to policy and procedures</p> <p>e) Capability to confirm expected results adhere to requirements intent</p> <p>f) Experience in process and procedure for auditing purposes</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</p> <p>c) Shall be onsite ninety percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<b>QA Analyst 1</b>	<p>a) Shall create test cases based on requirements with assistance of the QA Analyst 2</p>	<p>a) A minimum of 1 year of experience</p> <p>b) Capable of creating test cases with minimal assistance</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred</p>

Position	Description	Qualifications	Requirements
	<ul style="list-style-type: none"> <li>b) Shall assure requirements traceability to test cases</li> <li>c) Shall execute test cases</li> <li>d) Shall verify capture and retention of testing artifacts for audit purposes.</li> <li>e) Shall be responsible for assisting with the development and maintenance of the SOP manual.</li> </ul>	<ul style="list-style-type: none"> <li>c) Experience in executing test cases and validating and verifying results</li> <li>d) Experience in capturing test artifacts for auditing purposes</li> </ul>	<ul style="list-style-type: none"> <li>percent (100%) allocated to the project through Implementation and O&amp;M.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>
<b>Change Manager</b>	<ul style="list-style-type: none"> <li>a) Shall work with the State and HCFA Technical Change Control Board to ensure that IT changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner</li> <li>b) Shall be responsible for assisting with the development and maintenance of the SOP manual.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience as a Change Manager</li> <li>b) Experience leading Technical Change Control meetings</li> <li>c) Extensive knowledge of ITIL principals</li> <li>d) High level of IT literacy</li> <li>e) Superior attention to detail and methodical approach</li> <li>f) Excellent written and verbal communication at all organizational levels</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</li> <li>b) Shall be onsite ninety percent (90%) of the time</li> </ul>
<b>Service Architect</b>	<ul style="list-style-type: none"> <li>a) Responsible for assessing and designing complex solutions to meet the State's technology and business needs</li> <li>b) Shall manage project teams that consult with the State to analyze and identify technical requirements</li> <li>c) Shall manage requirements and project scope while meeting State expectations</li> <li>d) Shall provide level of effort estimates for deliverables, project sizing, and generating proposals</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of three (3) years' experience</li> <li>b) Demonstrated capabilities in leading technical projects with large, enterprise organizations</li> <li>c) Proven ability to provide a high level of capability with respect to service management, IT Service Management toolsets, service architecture, and business services</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</li> <li>b) Shall be onsite ninety percent (90%) of the time</li> </ul>
<b>IT Service Continuity Analyst</b>	<ul style="list-style-type: none"> <li>a) BC/DR Planning</li> <li>b) Risk Management</li> <li>c) Recovery Exercises</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience in a service continuity role.</li> <li>b) Experience in a large-scale mission critical environment.</li> <li>c) Must possess general knowledge with solutions utilizing an integrated development environment, multi-tier platforms and</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety</li> </ul>

Position	Description	Qualifications	Requirements
		<p>employing SOA architecture with high availability/reliability requirements.</p> <p>d) Must be proficient in multiple languages, SOA technologies, operating systems and security best practices.</p>	<p>percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<p><b>Senior Operations Analyst (Service Desk)</b></p>	<p>a) Monitor 7/24/365 and ensure reliability and availability for multiple system platforms including infrastructure, databases, backups, trouble shooting, problem resolution, escalation, and notification.</p> <p>b) Schedule and coordinate system installs, upgrades and outages.</p> <p>c) Establish priority problem resolution, notification and escalation to appropriate support personnel.</p> <p>d) Monitor and administer support and services for all Production Control, Service desk, and operations activities including perform all batch scheduling, production activities, printing, and print distribution.</p> <p>e) Setup, coordinate, and execute production batch schedules using automated job scheduling</p> <p>f) Analyze the production cycle and corresponding output to identify issues</p> <p>g) Communicate with internal teams and external customers to resolve issues</p> <p>h) Ensure accurate and timely transmission of secure data files to/from business partners via FTP and Contractor interface management\</p> <p>i) Shall be responsible for assisting with the development and</p>	<p>a) A minimum of three (3) years' experience in an operational or help desk position</p> <p>b) Excellent problem solving skills</p> <p>c) Excellent job scheduling activities</p> <p>d) Quality focus</p> <p>e) Experience with process improvement</p> <p>f) Ability to establish good client relationships</p> <p>g) Reporting skills</p> <p>h) Shall possess advance skills in batch scheduling activities</p> <p>i) Shall have extensive experience with operating systems and system administration</p> <p>j) Understanding of networking concepts and IT knowledge</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</p> <p>c) Shall be onsite ninety percent (90%) of the time.</p>

Position	Description	Qualifications	Requirements
<b>Operations Analyst (Service Desk)</b>	<p style="text-align: center;">maintenance of the SOP manual</p> <ul style="list-style-type: none"> <li>a) Monitor 7/24/365 and ensure reliability and availability for multiple system platforms including infrastructure, databases, backups, trouble shooting, problem resolution, escalation, and notification.</li> <li>b) Schedule and coordinate system installs, upgrades and outages.</li> <li>c) Establish priority problem resolution, notification and escalation to appropriate support personnel.</li> <li>d) Monitor and administer support and services for all Production Control, Service desk, and operations activities including perform all batch scheduling, production activities, printing, and print distribution.</li> <li>e) Setup, coordinate, and execute production batch schedules using automated job scheduling</li> <li>f) Analyze the production cycle and corresponding output to identify issues.</li> <li>g) Communicate with internal teams and external customers to resolve issues.</li> <li>h) Ensure accurate and timely transmission of secure data files to/from business partners via FTP and Contractor interface management.</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of two (2) years' experience in an operational or help desk position</li> <li>b) Excellent problem solving skills</li> <li>c) Quality focus</li> <li>d) Experience with process improvement</li> <li>e) Ability to establish good client relationships</li> <li>f) Reporting skills</li> <li>g) Shall possess advance skills in batch scheduling activities</li> <li>h) Understanding of networking concepts and IT knowledge</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> </ul>
<b>Incident/Problem Manager</b>	<ul style="list-style-type: none"> <li>a) Shall drive the efficiency and effectiveness of the incident/problem management process.</li> <li>b) Shall produce management information, including KPIs and</li> </ul>	<ul style="list-style-type: none"> <li>a) Minimum of five (5) years' experience in an Incident/Problem Management role for a large scale, mission critical environment</li> <li>b) Proven leadership and coaching skills</li> <li>c) Must be ITIL certified.</li> <li>d) Excellent problem solving and analysis skills</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</li> <li>b) Shall be onsite one hundred percent (100%) of the time</li> </ul>

Position	Description	Qualifications	Requirements
	<p>reports.</p> <p>c) Shall monitor the effectiveness of incident/problem management and making recommendations for improvement.</p> <p>d) Shall develop and maintain the incident/problem management system.</p> <p>e) Shall drive, develop, manage, and maintain the major incident/problem management process and associated procedures.</p> <p>f) Shall ensure that all IT teams follow the incident/problem management process for every incident.</p> <p>g) Shall be assist with the development and maintenance of the SOP manual.</p>	<p>e) Good understanding of network and IT knowledge</p>	
<b>IT Engineer/Systems Monitoring Analyst</b>	<p>a) Works under the supervision of the CIP Manager.</p> <p>b) Shall be proficient with monitoring tools management.</p> <p>c) Shall be proficient with Reports &amp; Dashboards.</p> <p>d) Shall be proficient with alerts configuration and management (metrics, thresholds, KPIs, etc.)</p> <p>e) Shall be proficient with trend Analysis (vulnerability, capacity, performance, and availability).</p> <p>f) Shall be proficient with Qualitative and Quantitative Analysis.</p> <p>a) Shall be responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>a) Minimum five (5) years' of technical support in a data center/service desk/network operations center.</p> <p>b) Extensive experience with industry standard monitoring tools.</p> <p>c) Must have extensive programming language skills</p> <p>a) Must have broad technical background in all areas of IT.</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be allocated one hundred percent (100%) to the project through O&amp;M.</p> <p>a) Shall be on site ninety percent (90%) of the time.</p>
<b>Principal Systems Security Officer (SSO)</b>	<p>b) The Principal SSO will manage the Medicare system security program and ensure the implementation of necessary</p>	<p>d) Must have a minimum of ten (10) years' experience in managing a large scale Medicare system security program</p>	<p>e) Shall not serve in any other position.</p> <p>f) Shall be allocated one hundred percent (100%) to</p>

Position	Description	Qualifications	Requirements
	<p>safeguards. The SSO should be organizationally independent of IT operations and cannot have responsibility for operation, maintenance, or development.</p> <p>c) Shall be assist with the development and maintenance of the SOP manual.</p>		<p>the project through Implementation.</p> <p>g) Shall be on site ninety percent (90%) of the time</p> <p>h) Shall be available as needed post Go-Live.</p>
<b>Security Architect</b>	<p>a) Shall research and advise the State on emerging technologies, trends, and leading practices as they pertain to enabling technology for eligibility modernization.</p> <p>b) Shall determine security requirements by evaluating business strategies and requirements and information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; and preparing cost estimates.</p> <p>c) Responsible for planning the security systems by evaluating network and security technologies; developing requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related security and network devices; evaluating the design of public key infrastructures (PKIs), including use of certification authorities (Cas) and digital signatures as well as hardware and software; and adhering to industry standards.</p> <p>d) Responsible for defining security</p>	<p>a) Possess a minimum of five (5) years industry experience with a strong preference towards healthcare environments.</p> <p>b) Possess a minimum of six (6) years on at least four (4) or more of the following security functional areas: credential management, access provisioning, authentication and authorization, access governance, application security, penetration testing, infrastructure security, data security, and security monitoring</p> <p>c) Possess a Bachelor's Degree in computer science OR four (4) years of industry experience in addition to the general requirement for two (2) years of security experience.</p> <p>d) Must be familiar with at least one major recognized architecture framework</p> <p>e) Must have excellent communications skills, writing skills, analytical skills, small group facilitation skills, and formal presentation skills</p>	<p>a) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</p> <p>b) Shall be onsite ninety percent (90%) of the time.</p>

Position	Description	Qualifications	Requirements
	<p>boundaries for the project as required and approved by the State.</p> <p>e) Accountable for delivering security architecture artifacts and deliverables as defined by the project SDLC.</p>		
<b>Senior Security Engineer</b>	<p>a) Responsible for penetration testing, cross script testing, perimeter testing, denial of service, etc.</p> <p>b) Responsible for validation and verification of firewall settings.</p> <p>c) Collaborate, review and approve security infrastructure effectiveness with the State and STS.</p> <p>d) Responsible for vulnerability management</p>	<p>a) Practical experience with DISA STIGS.</p> <p>b) Minimum of five (5) years' experience in security testing.</p> <p>c) Desired relevant professional information security certification.</p>	<p>a) Shall be fifty percent (50%) allocated to the project through Implementation and O&amp;M.</p> <p>a) Shall be onsite ninety percent (50%) of the time</p>
<b>Senior Security Analyst</b>	<p>a) Shall work closely with leadership and staff to identify, analyze, manage, and mitigate information security risk.</p> <p>b) Responsible for security monitoring activities.</p> <p>c) Responsible for development of compliance responses to regulatory authorities (e.g. CMS, SSA, State of TN, etc.)</p> <p>d) Shall identify, manage and escalate security incidents.</p> <p>e) Shall be responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>a) Minimum of five (5) years' related experience in a large scale mission critical environment.</p> <p>b) At least one relevant professional information security certification required: CISSP, CISM, CRISC, SANS, GIAC, or similar.</p> <p>c) Extensive experience dealing with sensitive data information systems.</p>	<p>d) Shall not serve in any other position.</p> <p>e) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</p> <p>f) Shall be onsite ninety percent (90%) of the time.</p>
<b>Security Analyst</b>	<p>a) Shall assist to identify, analyze, manage, and mitigate information security risk.</p> <p>b) Responsible for security monitoring activities.</p> <p>c) Responsible for assisting in the development of compliance</p>	<p>a) Minimum of two (2) years' related experience in a large scale mission critical environment</p> <p>b) Desired relevant professional information security certification: CISSP; CISM; Certified in Risk and Information Systems Control; SysAdmin, Audit, Network, and Security Institute; GIAC; or similar</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be one hundred percent (100%) allocated to the project through O&amp;M.</p> <p>c) Shall be onsite ninety percent (90%) of the time</p>

Position	Description	Qualifications	Requirements
<b>Privacy/Compliance Specialist</b>	<p>responses to regulatory authorities (e.g. CMS, SSA, State of TN, etc.)</p> <p>a) Responsible for overseeing activities related to the development, implementation, and O&amp;M of the eligibility Solution in compliance with State and Federal regulations and policies applicable to the privacy of and access to the sensitive data of the applicants, members insured, and members of the State work force.</p> <p>b) Responsible for Privacy Impact Analysis.</p> <p>c) Responsible for identifying, facilitating, and coordinating data classification activities.</p> <p>d) Assisting with privacy incident responses.</p>	<p>c) Extensive experience dealing with sensitive data information systems</p> <p>a) Possess a minimum of five (5) years of IT security industry experience with at least three (3) years in a healthcare related environment.</p> <p>b) Must be familiar with at least one major security compliance framework and be able to demonstrate a firm understanding of relevant State and Federal security/privacy regulations and policies, specifically under NIST, HIPAA, and IRS Pub. 1075</p> <p>c) Must possess working knowledge of solutions utilizing an integrated development environment, multi-tier platforms, and employing SOA.</p> <p>d) Must be familiar with multiple programming languages, SOA technologies, operating systems, and security industry standards.</p> <p>e) Must have successfully guided security compliance on at least one project with similar size and scope to the TEDS (e.g. Health Insurance Exchange, Integrated Eligibility or Medicaid Eligibility in other states) within the last five (5) years.</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be allocated one hundred percent (100%) to the project through Implementation and O&amp;M.</p> <p>c) Shall be on site ninety percent (90%) of the time.</p> <p>d) Shall be available as needed post Go-Live.</p>
<b>Output Document Manager</b>	<p>a) Manages end-to-end output document production.</p> <p>b) Responsible for day-to-day operational control.</p> <p>c) Responsible for meeting high paced production and delivery schedule.</p> <p>d) Responsible for assisting with the development and maintenance of the SOP manual.</p>	<p>a) Minimum of five (5) years' experience with Output Management, printers, Print technologies, mail management systems technologies and tools</p> <p>b) Shall have extensive experience with print technologies, high-speed printers, and spooling technologies</p> <p>c) Must have broad IT experience and background</p> <p>d) Experience managing an enterprise level, high volume, transactional document, output operation.</p> <p>e) Knowledge of USPS regulations and requirements regarding mail piece introduction into Postal mail stream.</p>	<p>a) Shall not serve in any other position.</p> <p>b) Shall be allocated one hundred percent (100%) to the project through O&amp;M.</p> <p>c) Shall be on site one hundred percent (100%) of the time</p>

Position	Description	Qualifications	Requirements
<b>Output Document Programmer</b>	<ul style="list-style-type: none"> <li>a) Responsible for designing, developing, creating, modifying and maintaining all output documents.</li> <li>b) Responsible for assisting with the development and maintenance of the SOP manual</li> </ul>	<ul style="list-style-type: none"> <li>f) Experience with mail-piece tracking solutions.</li> <li>a) Minimum of five (5) years' experience with forms design technologies and tools.</li> <li>b) Shall have extensive experience with print technologies, high-speed printers, and spooling technologies, mail management systems technologies and tools.</li> <li>c) Experience with industry standard document management applications</li> <li>d) Experience with transactional document development and creation to include template design and variable data insertion.</li> <li>e) Knowledge of USPS regulations and requirements regarding mail piece introduction into Postal mail stream.</li> <li>f) Experience with mail-piece tracking solutions.</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be allocated one hundred percent (100%) to the project through O&amp;M.</li> <li>c) Shall be on site one hundred percent (100%) of the time</li> </ul>
<b>Management and Administrative Support</b>	<ul style="list-style-type: none"> <li>a) Shall support operations by supervising staff and planning, organizing, and implementing administrative systems</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of five (5) years' experience in handling a wide range of operational and administrative related tasks</li> <li>b) Ability to work independently as well as work closely with the management team</li> <li>c) Must have exceptional verbal and written communication skills and a strong attention to detail</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall be one hundred percent (100%) allocated to the project through Implementation and O&amp;M.</li> <li>b) Shall be onsite ninety percent (90%) of the time</li> </ul>
<b>Technical Writer</b>	<ul style="list-style-type: none"> <li>a) Shall drive the creation of a documentation methodology and framework and maintain proper methodology for purposes of consistency and efficiency.</li> <li>b) Shall prepare and/or maintain documentation pertaining to programming, systems operation, and user documentation.</li> <li>c) Shall translate business specifications into user documentation.</li> <li>d) Shall assist with the development of the SOP manual.</li> <li>e) Shall be familiar with a variety of the field's concepts, practices,</li> </ul>	<ul style="list-style-type: none"> <li>a) A minimum of three (3) years' experience as a Technical Writer in a healthcare related business</li> <li>b) Good proofreading and editing skills</li> <li>c) Ability to convert technical knowledge into easily understood terms</li> </ul>	<ul style="list-style-type: none"> <li>a) Shall not serve in any other position.</li> <li>b) Shall be one hundred percent (100%) allocated to the project through Implementation.</li> <li>c) Shall be onsite ninety percent (90%) of the time.</li> <li>d) Shall be available as needed post Go-Live.</li> </ul>

Position	Description	Qualifications	Requirements
	and procedures		

## A.23 Facility

- A.23.1 The Contractor shall secure temporary office space within six (6) weeks of the start of the Contract. At the end of the six (6) week period, the Contractor shall have another six (6) weeks to secure a permanent facility sufficient to house its staff to fulfill the entire scope of this Contract. The facility shall be located within twenty-five (25) miles of the State offices located at 310 Great Circle Rd, Nashville, TN. All costs associated with the facility are the responsibility of the Contractor for the entire Contract period and such costs shall be factored into the Contractor's bid included in the maximum liability of the Contract and shall not be billed separately. The Contractor shall either directly house all necessary subcontractors or otherwise ensure the availability of necessary subcontractors to successfully complete the requirements of this Contract.
- A.23.2 The State may require certain Contractor personnel, as determined by the State, to work on-site at State offices at any point in the Contract, including during the time before the Contractor's temporary office space is secured.
- A.23.3 The Contractor staff shall be available for in-person meetings at the State office and at the Contractor's local office as needed. Meetings will be held at either the State's offices or the Contractor's local offices. Whenever appropriate meeting space is available at the State office, the meetings shall be held at the State offices. Should appropriate meeting space in the State's preferred office(s) be unavailable, the Contractor will provide appropriate meeting space.
- A.23.4 The Contractor shall provide the State with licenses for an industry standard teleconferencing service to allow for remote meetings. Meetings shall be held remotely at the sole discretion of the State.
- A.23.4.1 The Contractor shall leverage the State's video conferencing and collaboration licenses and tools (WebEx, Cisco TelePresence MX300 G2 and MX200 G2, etc.) where possible.
- A.23.5 The Contractor shall provide dedicated space for a minimum of ten (10) full time State staff and Contractors to be collocated with the Contractor and provide additional hoteling spaces as needed.
- A.23.5.1 The Contractor shall provide parking locations for State staff and State contractors at no additional cost to the State.
- A.23.6 The Contractor shall be responsible for providing State approved training facilities in accordance with the specifications and requirements set forth by the State and OCMT Team.
- A.23.7 Nothing in this agreement shall permit the Contractor's employees, agents, representatives, or sub-contractors to share, store, access, use, transport, or disclose State data in any form via any medium, including with any third parties, beyond the boundaries and jurisdiction of the United States of America without express written authorization from HCFA.
- A.23.8 Nothing in this agreement shall permit the Contractor's employees, agents, representatives, or sub-contractors to perform DDI or O&M activities on the Solution beyond the boundaries and jurisdiction of the United States or to leverage systems infrastructure, components, or resources that are hosted beyond the boundaries and

jurisdiction of the United States in support of these activities without express written authorization from HCFA.

#### A.24 Status Performance Reporting

A.24.1 Status and performance of the program shall be reported on by the Contractor to establish effective program communication to all stakeholders. The Contractor shall provide the State with Program Status Reports outlining progress against key milestones, assessing scope, schedule, budget, resources, and quality and identifying project risks and issues. In addition, the Contractor shall produce performance reports on an ongoing basis and provide reports that communicate key program metrics including, but not limited to, cost, schedule, budget, and testing. The Contractor shall produce each report type in compliance with the frequency, audience and stakeholder needs, and report delivery methods established by the State for the report type. The primary audience for the reports includes, but is not limited to the following recipients: The Project Steering Committee, State Program Director, SPMO Contractor, and TAS Contractor. The table below provides more information about reporting requirements and includes the medium in which the Contractor shall deliver the report. The list, and the respective report's contents, is subject to change at the State's discretion.

*Table 4: Status and Performance*

Report/Meeting Name	Frequency	Level and Internal or External Intent	Method	Reporting Elements
<b>Executive Steering Committee Meeting</b>	Monthly	Program/External	Written materials delivered in presentation	Program status, progress towards roadmap and overall outcomes, Items requiring decisions, Key risks & issues, Open Project Procurements Status, Project Advance Planning Document Status, Open Project Recruiting Status, Monthly State & Federal Agency/Committee Communications Log Changes, Communication Plan Status, Document Management
<b>Contractor Status Report Meeting</b>	Biweekly	Program/External	Live Meeting/Written materials delivered in presentation	Status, progress toward roadmap and overall outcomes, items requiring decisions, key issues/risks for management attention
<b>Contractor Risk, Issues, and Action Items Focus Meeting</b>	Biweekly	Program/External	Live Meeting/Written materials	In depth discussion of key project risks, issues and action items
<b>Contractor State Business Owners Status Report Meeting</b>	Biweekly	Project/External	Written materials delivered in presentation	Project status, items requiring decisions, key risks/issues and action items relative to the project
<b>CIO Status Report Meeting(s)</b>	Weekly	Program/External	Written materials delivered in presentation	Project status, progress, key issues/risks for management attention
<b>Contractor Testing Status</b>	Weekly	Project/Internal	Written Materials	Project status, progress, key issues/risks, key successes

Report/Meeting Name	Frequency	Level and Internal or External Intent	Method	Reporting Elements
<b>Report Meeting</b>				
<b>Contractor Quality Management Status Report Meeting</b>	Monthly	Program/External	Written Materials	QM project status and risk overview, key milestones, development of key initiative project deliverables, planned versus actual and critical path analysis, assessment of the EMP work plan, project plan critical path, risk/issue assessment
<b>SDLC Status Meeting</b>	Biweekly	Program/External	Written, Web Pages, and Query Tool	Status of architecture artifacts during the SDLC.
<b>Contractor Testing Meeting</b>	Weekly	Program/External	Written Results of the Test	Contractor test planning status, testing outcomes, potential issues or problems from testing for leadership attention
<b>Program Status Report</b>	Biweekly	Program for all Projects/External	Written	Dashboard-style assessment of program status including milestone status and accomplishments, KPI and supporting metrics, new issues and risks, accomplishments this period, plans for next period, and key decisions, focusing Steering Committee on key issues for management attention.
<b>Risk &amp; Issue Log</b>	Weekly	Program (Identifiable by project)	Written	Risks/Issues across all initiatives, overall assessment, trends, and resolution
<b>Quality Risk Management Status Report</b>	Monthly	Project/External	Written	Dashboard-style assessment of project status, focuses Steering committee on key issues for management attention
<b>CMS Status Report</b>	Monthly	External	Written	Dashboard-style assessment of project status, focuses Steering committee on key issues for management attention
<b>Contractor Testing Status Report</b>	Weekly	Project/Internal	Written	Dashboard-style assessment of the testing successes and risks related to the specific projects
<b>Contractor System Deliverables Report</b>	Biweekly	Project/External	Written	Dashboard-style assessment of the deliverables status related to the specific projects
<b>Contractor Systems Retirement Report</b>	Biweekly	Project/External	Written	Dashboard-style assessment of the retirement and transition status of legacy systems related to the specific projects
<b>Contractor Daily/Monthly Operations Reports</b>	Daily	Project/External	Written	Interface events and issues, System events and issues, Software events and issues, Errors and Anomalies, Transactions Sent and Received (Daily and Total Amount), Transaction Types, Staffing and Operational Activities and Issues, Number of notices and letters received and sent (including any and all reconciliation efforts), audit tracking of letter/notices by page, Cumulative statistics, Performance against Service Level Agreements, and complete breakdown of all letters and notices by type.
<b>Contractor</b>	Weekly	Project/External	Written	Action plans, implementation of

Report/Meeting Name	Frequency	Level and Internal or External Intent	Method	Reporting Elements
Root Cause Analysis Report		nal		solution/workaround
Contractor Turnover Status Reports	Monthly	Project/External	Written	Documentation of turnover plans for business operations and system operations
Contractor SLA Report	Monthly	Project/External	Written	Automated performance report, prior month performance of each service against all of its respective KPIs
CIP Meeting	Quarterly	Program/External	Written	Solution health status, capacity, metrics, KPIs, infrastructure issues/concerns,, corrective actions, gaps, future state, optimization improvement, etc.
Technical Change Control Board Meeting	Biweekly	Project/External	Live Meeting/Written materials delivered in presentation	Existing technical change control items for review
Technical Infrastructure Touch Point Meeting	Weekly	Project/External	Written materials delivered in presentation	Project status, progress, key issues/risks, key successes

#### A.25 Work Product and Hardware Ownership

A.25.1 Contractor shall assign, transfer and convey to the State all right, title and interest in all Work Product, as defined in Section E.4.a.5 of this Contract and all hardware developed, procured or managed by the Contractor as required by this Contract. Contractor shall also provide a document of the inventory of all Work Product and hardware developed, procured or managed by the Contractor as required by this Contract and specify that the supplied components and materials are current, accurate, and complete.

A.25.2 The Contractor shall assign, transfer, and convey to the State all right, title, and interest in the following upon implementation of each Release of the TEDS:

A.25.2.1 Software Code

A.25.2.2 Intellectual Property for COTS customizations

#### A.26 Warranty

##### A.26.1 Warranty Period

A.26.1.1 The Contractor shall provide a warranty period, whereby any defects identified during this period must be resolved within a timeframe defined by the State, with no additional cost to the State or need for project change control processing.

A.26.1.2 The Contract shall provide a warranty period of six (6) months for each release of the Solution upon deployment in the production environment.

A.26.1.3 Warranty defects shall be classified as critical, high, medium and low as described in Contract Attachment 2 – Liquidated Damages.

- A.26.1.4 The identification of critical and high defects of the Solution during the Warranty Period shall extend the warranty period for the Solution for six (6) months after the time of resolution of critical or high defects.
  - A.26.1.5 The warranty period shall begin only after the resolution of all defects identified prior to the Go-Live of that release.
  - A.26.1.6 In the event that a subsequent Release creates or identifies defects in the deployed Solution, the Warranty period of the created or identified defect will be covered by the warranty of that subsequent Release.
  - A.26.1.7 The Contractor shall warranty that each release of the Solution implementation conforms to system requirements and expected outcomes as detailed in the functional design documentation, technical design documentation, and System Security Plan as approved by the State.
  - A.26.1.8 The Contractor shall warranty that each subsequent Solution implementation will build upon and conform to previously released functionality, unless a change is explicitly approved by the State.
  - A.26.1.9 The Contractor shall be responsible for resolving any and all warranty defects at no additional cost to the State. This includes defects identified within the new release, as well as newly identified defects that have caused previously functioning components of the Solution to work incorrectly.
  - A.26.1.10 The term of the Warranty survives the termination of the contract. If warranty work will occur after Turnover of the Solution, the Contractor shall include warranty deliverables, testing, etc. as part of the Turnover Plan.
- A.26.2 Documentation and Resolution of Warranty Defects
- A.26.2.1 The Contractor shall define a process to classify and track defects that trigger the warranty provisions in Section A.26.
  - A.26.2.2 The Contractor shall be responsible to resolve all critical and high warranty defects within the periods described in Contract Attachment 2, or, if necessary, provide the State with a mutually acceptable written work-around, downstream impacts, and plan for resolution, all without additional cost to the State.
  - A.26.2.3 The Contractor shall resolve all medium and low defects within sixty (60) days of identification.
  - A.26.2.4 The Contractor shall be subject to corresponding Liquidated Damages, listed in Contract Attachment 2, for all identified warranty defects that are not resolved within the associated resolution timeframes.
- A.27 Table of Deliverables
- A.27.1 The Contractor shall complete the following deliverables for each of the Scope of Work sections above, as indicated in the Table below.
  - A.27.2 The Contractor shall ensure each deliverable's compliance with the appropriate and corresponding State plan, where applicable.

- A.27.3 Where identified deliverables require ad hoc updates or are updated periodically during the course of the implementation:
- A.27.3.1 The Contractor shall update content in the original deliverable. Updated content provided in a Deliverable Amendment (and not integrated into the original deliverable) requires prior authorization by the State.
  - A.27.3.2 The Contractor's completion of, and the State's acceptance of, a deliverable during one Gate Review does not constitute acceptance of that deliverable for any subsequent Gate Review.

Table 5: Deliverables

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
Deliverable 1	Project Management Plan	Once upon State approval;  Update if necessary	The Project Management Plan is the overall plan for project execution, monitoring, and control and should include information describing the project management approach, the internal organizational structure and organizational chart, roles and responsibilities, a summary of the Project's purpose, scope, and objectives, a description of an the constraints and/or assumptions on which the Project is based, a list of product deliverables, a summary of the Project's schedule and budget, and the methods for updating, reviewing and disseminating the PMP as well as specific supplemental management plans for critical project areas: <ul style="list-style-type: none"> <li>a) Overall Project Management Approach</li> <li>b) Scope Management Plan</li> <li>c) Schedule Management Plan</li> <li>d) Communication</li> </ul>	<ul style="list-style-type: none"> <li>a) The Project Management Plan and component plans have been reviewed and appropriately updated.</li> <li>b) The Project Management Plan defines how the project will be executed, monitored and controlled and includes high level estimates of the baselines.</li> <li>c) The Project Management Plan is fully scaled and details all the appropriate components that address the needs of the project. This includes the definition of appropriately scaled reviews and deliverables</li> </ul>	<ul style="list-style-type: none"> <li>a) Issues List</li> <li>b) Action Items</li> <li>c) Decision Log</li> <li>d) Lesson Learned Log</li> <li>e) Staff Planning and Monitoring Processes</li> <li>f) Staffing Tracker</li> <li>g) Resource Availability Calendar</li> <li>h) Key Personnel Transition Plan</li> <li>i) Onboarding Checklist</li> <li>j) Onboarding Arrival Packet</li> <li>k) Acceptable Use Policy and Information Protection Plan</li> <li>l) Roll-On Form</li> <li>m) Team Member Transitions Plan</li> <li>n) Roll-Off Form</li> <li>o) Off-Boarding Checklist</li> </ul>	Type C	A.8

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			Management Plan e) Quality Management Plan f) Risk/Issue Management Plan g) Change Management Plan (including Training Plan) h) Configuration Management Plan i) Performance Management Plan j) Staffing Management Plan k) Financial Management Plan  The Project Management Plan is created during the PBR Gate of the SDLC and State approval of the project management plan is required as a criteria item for completion of the Project Baseline Review				
<b>Deliverable 2</b>	Key Performance Indicator Management Plan	Once upon State approval;  Update if necessary	The KPI Management Plan describes the processes and mechanisms by which Key Performance Indicators will be defined, tracked, and properly reviewed during the	a) The Plan properly describes the state-approved KPIs that will be tracked during the project	a) Continuous Improvement Plan	Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>duration of the project. At a minimum the KPI Management Plan shall include:</p> <ul style="list-style-type: none"> <li>a) A description of the KPI, and the business value it will bring to the project</li> <li>b) Identification of the tools, processes, inputs, and calculations that will be used to generate the KPIs current result</li> <li>c) The process by which KPIs will be reported, tracked, and reviewed to ensure that over time the KPI is in compliance with established limits</li> <li>d) Additional metrics that will be needed for each KPI if is found out of compliance</li> <li>e) The communication plan for reporting KPI results, including escalation plans</li> </ul>	<ul style="list-style-type: none"> <li>b) The Plan establishes the process by which KPIs will be documented, tracked, and updated over time</li> <li>c) The Plan details how each KPI will be calculated</li> <li>d) The Plan has a properly defined KPI communication plan</li> </ul>			

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			for KPIs found out of compliance f) The roles and responsibilities for KPI generation, tracking, and reporting				
<b>Deliverable 3</b>	Requirements Management Plan	Once upon State approval;  Update if necessary	The Requirements Management Plan provides a clear and concise layout of how detailed requirements will be gathered (including sections for functional, technical, security, performance, operational, etc.).  The Requirements Management Plan must outline a robust method to store and track functional, technical and other operational and performance requirements.	a) The Requirements Management Plan prescribes the tools and methodologies of capturing, standardizing, classifying, monitoring, reporting, maintaining, and managing requirements.  b) The Requirements Management Plan shall outline methods for maintaining requirements traceability throughout the development process; methodology and processes adopted during development; types and conduct of test activities, and		Type A	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				the change control and configuration management processes.			
<b>Deliverable 4</b>	Business Rules Management Plan	Once upon State approval;  Update if necessary	The Business Rules Management Plan will detail the tools, processes, and methods by which business rules are managed, changed, or retired.	<ul style="list-style-type: none"> <li>a) The Business Rules Management Plan outlines the standards, tools, and methodologies that will be used in managing business rules across the solution life cycle.</li> <li>b) The Business Rules Management Plan outlines the industry-recognized Business Rules Engine (BRE) or Business Rules Management System (BRMS) used to document business rules</li> <li>c) The Business Rules Management Plan outlines the format that will be utilized when developing business rules</li> <li>d) The Business</li> </ul>		Type A	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>Rules Management Plan identifies the responsibilities of Business Rules Management, including critical access and segregation of duties considerations</p> <p>e) The Business Rules Management Plan includes explanation regarding compliance with the Minimum Acceptable Risk Standards for Exchanges (MARS-E), and proper alignment with the project Security Plan</p>			
<b>Deliverable 5</b>	Design Management Plan	Once upon State approval;  Update if necessary	The Design Management Plan details the approach to system design. The plan must ensure that the system conforms to the defined standards for system design and systems architecture. The plan also ensures that the Enterprise Architecture (EA) requirements within the State are taken into consideration during the	<p>a) The Design Management Plan details the approach to system design.</p> <p>b) The Design Management Plan must ensure that the system conforms to the defined standards for</p>		Type A	A.27

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			System design. The plan must ensure completeness and level of detail in design specifications. The Design Management Plan will outline considerations of the design on the selection of a Software Development Methodology.	<ul style="list-style-type: none"> <li>c) The Design Management Plan demonstrates conformance to the States Enterprise Architecture (EA).</li> <li>d) The Design Management Plan demonstrates how all requirements will be addressed in design.</li> <li>e) The Design Management Plan must ensure completeness and level of detail in design specifications.</li> <li>f) The Design Management Plan will outline considerations of the design on the selection of a Software Development Methodology.</li> </ul>			
<b>Deliverable 6</b>	Test Management Plan	Once upon State approval;	The Test Management Plan outlines the approach that will be	<ul style="list-style-type: none"> <li>a) The Test Management Plan details the</li> </ul>	<ul style="list-style-type: none"> <li>a) Unit Testing template</li> <li>b) Smoke/Sanity</li> </ul>	Type A	A.10 A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
		Update if necessary	employed to test the Solution and to evaluate the results of that testing; outlines general testing roles and responsibilities; and serves as the top-level plan that will be used to govern and direct the detailed testing work. The Test Management Plan should address complexities associated with a multiple release implementation.	<p>planning, execution, and management activities to be executed in order to monitor and control testing, and ensure alignment of corresponding activities with the project goals and objectives.</p> <p>b) The Test Management Plan references a defect resolution process that is inclusive of defect identification, prioritization, creation, tracking, and resolution and retesting activities to be followed when a defect is found.</p> <p>c) The Test Management Plan defines the testing environments hours of operations during testing execution.</p> <p>d) The Test</p>	<p>Testing template</p> <p>c) Regression Testing template</p> <p>d) Ad-hoc Testing template</p> <p>e) Exploratory Testing template</p> <p>f) Usability Testing template</p> <p>g) GUI Software Testing template</p> <p>h) Accessibility Testing template</p> <p>i) Security Compliance Testing template</p> <p>j) Compatibility Testing template</p> <p>k) Functional Testing template</p> <p>l) Boundary Testing template</p> <p>m) Negative Testing template</p> <p>n) Error Handling Testing template</p> <p>o) Alert/Monitoring Testing template</p> <p>p) Capacity Testing template</p> <p>q) Performance Test Plan and Results template</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				Management Plan outlines the expectations for level of detail that shall be required in each test case.			
<b>Deliverable 7</b>	Implementation and Deployment Plan	Monthly, throughout project lifecycle	The Implementation and Deployment Plan explains the implementation methodology to be used, explaining how operations will transfer from the legacy system to the new System. The Plan will also contain an up-to-date detailed implementation schedule.	<ul style="list-style-type: none"> <li>a) The Implementation and Deployment Plan contains an up-to-date detailed implementation schedule to be followed.</li> <li>b) The Implementation and Deployment Plan describes the major tasks required to be taken, and the objective behind each task.</li> <li>c) The Implementation and Deployment Plan lists the support equipment (hardware), software, data, facilities and materials required for the implementation, if applicable.</li> </ul>	<ul style="list-style-type: none"> <li>a) Release Plan</li> <li>b) Implementation Plan</li> <li>c) Monitoring Strategy</li> <li>d) Version Description Document</li> <li>e) Information System Description</li> <li>f) Release and Deployment Plan</li> <li>g) System Sunset Plan</li> <li>h) Cut-Over Plan</li> <li>i) Roll Back Plan</li> <li>j) Turnover Plan</li> <li>k) Knowledge Transition Plan</li> </ul>	Type A	A.10 A.17
<b>Deliverable 8</b>	Data Conversion and	Monthly, throughout project	The Data Conversion and Synchronization Plan describes the strategy,	<ul style="list-style-type: none"> <li>a) The Data Conversion and Synchronization</li> </ul>	<ul style="list-style-type: none"> <li>a) Extract Control Documents</li> </ul>	Type A	A.14

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
	Synchronization Plan	lifecycle	preparation, and specifications for data conversion activities. This plan describes the overall approach, assumptions, and processes that will be used in the data conversion. It includes an inventory and cross reference of source and target data elements, schema, metadata and all self-describing files; process for data extraction, transformation and loading for each data source; tools needed to execute the conversion; and strategy for data quality assurance and control.	<p>Plan describes rationale for the conversion and a general description of the boundaries of the data conversion effort</p> <p>b) The Data Conversion and Synchronization Plan outlines the approach that will be used to extract, transform/cleanse and load data from the source to target destinations during the conversion/migration process</p> <p>c) The Data Conversion and Synchronization Plan outlines the schedule of conversion activities to be accomplished in accordance with this Data Conversion Plan</p>	b) Roll Back Plan		
<b>Deliverable 9</b>	System Security Plan	The initial System Security Plan shall be completed in Release I then	The System Security Plan documents the system's security level and describes managerial, technical and operational security controls. An Initial copy of the System	a) The System Security Plan works in synchronization with the safeguard procedures to	<p>a) Part A System Identification</p> <p>b) Part B Security Controls Workbook</p> <p>c) Part C Privacy</p>	Type C	A.19 A.26

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
		reviewed and updated on an as needed basis, including annually, and when there are major system modifications that could potentially impact the security and privacy of the information system.	Security Plan includes an initial Risk Assessment (RA) that contains mission/business process risks and the monitoring strategy, for review and approval by the Technical Change Control Board (TCCB) and Project Steering Committee.	<p>detail the control requirements for the protection of all data received, stored, processed and transmitted in compliance with all Federal Laws and Regulations.</p> <p>b) The System Security Plan includes the current level of existing security controls within the System that protect the confidentiality, integrity and availability (CIA) of the system and its information.</p> <p>c) The System Security Plan outlines the applicable Laws or Regulations.</p> <p>d) The System Security Plan contains a review log that is maintained to record the reviews that have taken place for this system.</p> <p>e) The System Security Plan</p>	<p>Controls Workbook</p> <p>d) Part D SSP Attachments</p> <p>e) Appendix A – IRS Requirements for Safeguarding Federal Tax Information (FTI)</p> <p>f) Appendix B – Security and Privacy Agreements and Compliance Artifacts</p> <p>g) Memorandum of Understanding</p> <p>h) Interconnection Security Agreements (ISA)</p> <p>i) Computer Matching Agreement</p> <p>j) Information Exchange Agreement</p> <p>k) Privacy Impact Analysis</p> <p>l) Security Impact Analysis</p> <p>m) Asset Inventory</p> <p>n) Asset Management Plan</p> <p>o) Information System Risk Assessment</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				organizes security controls into groups of families. f) Exit criteria includes CMS signoff	(ISRA)		
<b>Deliverable 10</b>	Business Continuity and Disaster Recovery Plan	Monthly, throughout project lifecycle	The Business Continuity and Disaster Recovery Plan describes the strategy and organized course of action that is to be taken if things don't go as planned or if there is a loss of use of the established business product (e.g., system) due to a disaster such as a flood, fire, computer virus, or major failure. The Business Continuity and Disaster Recovery Plan describes the strategy for ensuring recovery of the business product in accordance with stated Recovery Time Objective and Recovery Point Objectives.	a) The Business Continuity and Disaster Recovery Plan b) The Business Continuity and Disaster Recovery Plan prescribes responsibilities as they relate to actions that will be taken in response to a disruption. c) The Business Continuity and Disaster Recovery Plan clearly outlines milestones, notification activities, emergency handling of routine procedures, required contacts, formal agreements, lessons learned activities, and procedures to return normal	a) Business Continuity Plan b) Disaster Recovery c) Disaster Recovery Plan Training d) Configuration Management Plan e) Configuration Management Database f) Asset Management Plan g) Business Continuity Plan Training h) Backup Management Plan i) Business Impact Analysis	Type A	A.10 A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				operations in the event of a disaster.			
<b>Deliverable 11</b>	Capacity Plan	Monthly, throughout project lifecycle	<p>The Capacity Plan will address business capacity, service capacity, and IT component capacity management strategies that will be executed through the duration of the project. The Capacity Plan will also outline the management process and tools that will be used to complete capacity management, as well as estimates of future system workloads.</p> <p>The capacity plan will include, but not limited to, infrastructure, database, network, and any other aspects required to meet the performance requirements of the system.</p>	<ul style="list-style-type: none"> <li>a) The Capacity Plan demonstrates a State-approved skill and resource level to effectively execute the Capacity Plan.</li> <li>b) The Capacity Plan defines capacity performance success at the business process level</li> <li>c) The Capacity Plan outlines the practices, objectives, performance factors, monitoring and reporting activities, and communication strategies of the Capacity Plan.</li> <li>d) The Capacity Plan addresses steps and activities needed to address instances of abnormal levels of system use outside of forecasted</li> </ul>	a) System Capacity and Performance Plan	Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				operating procedures.			
<b>Deliverable 12</b>	Data Management Plan	Monthly, throughout project lifecycle	A defined plan for the management of data that provides, at a minimum, a summary of activities for data generation, a summary of the types of data generated by the relevant activities, the plans for preservation of the generated data, and a description of the appropriate level of access for the generated data.	<ul style="list-style-type: none"> <li>a) The Data Management Plan includes a summary of activities that generate data</li> <li>b) The Data Management Plan includes a summary and appropriate categorization of the data types generated by the identified activities.</li> <li>c) The Data Management Plan includes a plan for storage and maintenance of the data generated by the identified activities, in both the short-term and long-term (if relevant).</li> <li>d) The Data Management Plan includes a plan describing whether and how the data generated by the identified activities will be reviewed and</li> </ul>		Type A	A.12

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				made available to the public and how the metadata describing it will be stored.			
<b>Deliverable 13</b>	Performance and Availability Plan	Monthly, throughout project lifecycle	The Performance and Availability Plan will identify target performance areas and methods of measurement; establish the baseline metrics for the agreed upon goal areas; and assist HCFA in determining the level of achievement of the performance goals.	<ul style="list-style-type: none"> <li>a) The Performance and Availability Plan identifies and prioritizes the performance measurement goals and objectives to align with the information needs of the customer, project, organization, and stakeholders, as applicable.</li> <li>b) The Performance and Availability Plan includes a Traceability of Information Needs to Measurement Objectives by defining the information need, measurement objective, and the performance measure threshold.</li> </ul>	<ul style="list-style-type: none"> <li>a) Performance Test Plan and Results Template</li> <li>b) Program Availability Management Plan</li> </ul>	Type A	A.10 A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<ul style="list-style-type: none"> <li>c) The Performance and Availability Plan describes the methods, processes, tools and techniques that will be used for performance measurement.</li> <li>d) The Performance and Availability Plan outlines the data that will be collected, how it will be collected, and where it will be stored.</li> <li>e) The Performance and Availability Plan includes analysis on the data collected, and a review of the data to identify trends and opportunities for improvements and corrective actions.</li> <li>f) The Performance and Availability Plan includes an approach for identifying and addressing deficiencies in</li> </ul>			

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				performance and availability.			
<b>Deliverable 14</b>	Work Breakdown Structure (WBS)	Monthly, throughout project lifecycle	<p>The Work Breakdown Structure (WBS) is a preliminary step in the preparation of a project work plan and schedule that encompasses all activities from Project Initiation to Project Closure. The WBS must define the project's overall objectives by describing the project tasks and deliverables. The WBS must include:</p> <ul style="list-style-type: none"> <li>a) A consolidated view of the activities, activity descriptions, and activity durations</li> <li>b) Resources assigned to each activity</li> <li>c) A list of deliverables tied to project milestones</li> <li>d) A way to track the project schedule against the planned schedule</li> <li>e) Deliverable approval periods</li> </ul> <p>This deliverable is associated with the PBR Gate and must be delivered to the State</p>	<ul style="list-style-type: none"> <li>a) The WBS defines 100% of the project scope</li> <li>b) The WBS was created with input provided by all relevant stakeholders</li> <li>c) The WBS is outlined as such that the project activities and tasks are able to be executed, monitored, and controlled.</li> <li>d) The WBS is broken down such that any work package greater than 80 hours must be broken down into component activities.</li> <li>e) The WBS includes a WBS Dictionary, or executable activities being followed to completing the process.</li> </ul>		Type A	A.8

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			prior to the completion of the project baseline review.				
<b>Deliverable 15</b>	Risk Register (update weekly)	Monthly, throughout project lifecycle	The Risk Register contains the findings of the Risk Management Process and serves as the source of record for risk management activities to track the approaches and action plans for dealing with identified risks, which typically involve one of four options: avoidance, mitigation, transference, or acceptance. Once an approach is selected, detailed actions to implement are developed and the risk register serves as a record of those activities that information throughout the SDLC. The initial risk register is created during the ORR Gate and must be approved by the state prior to the completion of the project baseline review.	<ul style="list-style-type: none"> <li>a) The Risk Register will contain Risk Category, Probability, Impact, Risk Score, Risk Ranking, Risk Response, Trigger and Risk Owner.</li> <li>b) The Risk Register should identify how risks are mitigated (change request, work around, deferment)</li> </ul>	a) Risk Management Plan	Type A	A.24
<b>Deliverable 16</b>	Baselined Work Plan and Schedule	Monthly, throughout project lifecycle	This is a work plan and schedule that is managed in an appropriate project management tool.	<ul style="list-style-type: none"> <li>a) The schedule has sufficient detail to support the projected durations.</li> <li>b) The master work plan must reflect any changes from the plan submitted within</li> </ul>		Type A	A.8

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				the Contractor's original proposal that were discussed and agreed to during project planning.			
<b>Deliverable 17</b>	Status Reporting	Weekly and Monthly, throughout project lifecycle	<p>This deliverable must be a recurring deliverable for the entire length of the project. The deliverable must at a minimum include periodic reporting of the following activities:</p> <ul style="list-style-type: none"> <li>a) Status of work completed against the Project Work Plan</li> <li>b) Objectives for the next reporting period</li> <li>c) Client responsibilities for the next reporting period</li> <li>d) Recovery plan for all work activities not tracking to the approved schedule</li> <li>e) Projected completion dates compared to approved baseline key dates</li> <li>f) Escalated risks, issues (including schedule and</li> </ul>	a) The reports contain all of the required elements as agreed upon by HCFA and the Contractor.		Type A	A.8 A.24

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>budget), and Action items</p> <p>g) Disposition of logged issues and risks</p> <p>h) Important decisions</p> <p>i) Actual/projected Project Work Plan dates versus baseline Project Work Plan milestone dates</p> <p>j) One-page graphical summary of the Project Work Plan status of all major tasks and subtasks for each release in a Desktop Project Plan</p> <p>Adjustments to status reporting requirements will be addressed through the Memorandum of Understanding (MOU) process.</p>				
<b>Deliverable 18</b>	Financial Status Report	Weekly and Monthly, throughout project lifecycle	The Financial Status Report tracks the project costs to the project budget baseline and outlines any budgetary risks.	<p>a) Includes estimates to completion, or cost performance index information.</p> <p>b) It will reflect approved changes to</p>		Type A	A.24

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<ul style="list-style-type: none"> <li>c) Includes reporting on any project work stream that has had activity against it.</li> </ul>			
<b>Deliverable 19</b>	Detailed Requirements Traceability Matrix	Updated monthly throughout project lifecycle	The Detailed Requirements Traceability Matrix describes the life of a requirement, in both a forward and backward direction, ideally through each step of the entire product's life cycle, ensuring scope is met.	<ul style="list-style-type: none"> <li>a) The Requirements Traceability Matrix outlines describes each requirement independently, which Release each requirement was met or updated, and provides traceability to applicable test cases to demonstrate how each requirement was implemented.</li> <li>b) The Requirements Traceability Matrix shows the difference between functional and non-functional requirements.</li> <li>c) The Requirements Traceability Matrix allows rationale to be included when</li> </ul>	<ul style="list-style-type: none"> <li>a) Requirements Specification Document including but not limited to:</li> <li>b) Business Rules</li> <li>c) Business Process Flow Diagrams</li> <li>d) Requirements Traceability Matrix Functional/Non-Functional Requirements</li> </ul>	Type C	A.12

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				requirements are not fully traceable throughout the lifecycle.			
<b>Deliverable 20</b>	Requirements Specification Document	Once per release upon State approval	The Requirements Specification Document provides all requirements expected to be implemented. This document lists the business requirements, business rules, stakeholder requirements, and functional/nonfunctional requirements for the project. It also contains use case scenarios that describe how the requirements will be implemented.	<ul style="list-style-type: none"> <li>a) The Requirements Specification Document outlines business, technical, governance and project management stakeholders inclusive of requirements gathering, review, and approval.</li> <li>b) The Requirements Specification Document includes references to all interdependent deliverables and artifacts throughout the lifecycle, specifically documents that ensure traceability to the implemented Solution.</li> <li>c) The Requirements Specification</li> </ul>	<ul style="list-style-type: none"> <li>a) Requirements Specification Document including but not limited to: <ul style="list-style-type: none"> <li>b) Business Rules</li> <li>c) Business Process Flow Diagrams</li> <li>d) Requirements Traceability Matrix Functional/Non-Functional Requirements</li> </ul> </li> </ul>	Type A	A.12

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>Document includes business and functional rationale of the included requirements.</p> <p>d) The Requirements Specification Document details the Solution, written in a level of detail easily understood by non-technical personnel.</p> <p>e) The Requirements Specification Document includes Business Process Flow Diagrams detailing the Business Process that is being introduced or enhanced.</p>			
<b>Deliverable 21</b>	System Architecture Design Document	Once per release upon State approval	The System Architecture Design Document (SADD) describes: <ul style="list-style-type: none"> <li>a) How the functional and nonfunctional requirements recorded in the Requirements Document will</li> </ul>	<ul style="list-style-type: none"> <li>a) Functional and non-functional requirements are mapped to supporting technical design.</li> <li>b) Functional design requirements are mapped to</li> </ul>	<ul style="list-style-type: none"> <li>a) Technical Architecture Diagrams</li> <li>b) Systems Design Document</li> <li>c) High Level Technical Design Concept/Alternat</li> </ul>	Type C	A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>b) How the preliminary user-oriented functional design recorded in the High Level Technical Design Concept/Alternatives document will be met in the Solution design.</p> <p>The SADD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level detailed design specifications for each of the system's components, including hardware, internal communications, software, system integrity controls, and external interfaces. The high-level system design serves as primary input to the Preliminary Design Review. The low-level detailed design serves as</p>	<p>c) A high level system design is provided.</p>	<p>d) FTI Labeling Methodology</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			input to the Detailed Design Review.				
<b>Deliverable 22</b>	Interface Control Document(s)	Once per release upon State approval	<p>The Interface Control Document (ICD) describes the relationship between the two interconnected systems. This ICD specifies the interface requirements to be met by the participating systems and at minimum, describe the interface definitions and design (including XML/SOAP/flat file/other specifications for file formats),. It describes the design specifications for the interface, defines the message structure and protocols that govern the interchange of data, and identifies the communication paths along which the data are expected to flow. For each interface, the following information will be provided:</p> <ul style="list-style-type: none"> <li>a) A general description of the interface;</li> <li>b) Assumptions where appropriate;</li> <li>c) A description of the data exchange format and protocol for exchange; and</li> </ul>	<ul style="list-style-type: none"> <li>a) All ICDs defined as required have been created.</li> <li>b) The ICD describes the interface, including purpose, format, message structure, and protocols.</li> <li>c) The ICDs indicate the size and frequency of the data exchange.</li> <li>d) Memorandum of Understanding or System Interface Agreements have been established to document the interface expectations.</li> <li>e) The ICD has been tested via simulation.</li> </ul>	<ul style="list-style-type: none"> <li>a) TEDS Interface/Integration Management Plan</li> <li>b) Memorandum of Understanding</li> <li>c) Interconnection Security Agreement</li> <li>d) Interface Control Test Plan</li> </ul>	Type C	A.10 A.16

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			d) Estimated size and frequency of data exchange				
<b>Deliverable 23</b>	Database Design Document	Once per release upon State approval	The Database Design Document describes the design of a database and the software units used to access or manipulate the data.	<ul style="list-style-type: none"> <li>a) The Database Design Document outlines the DBMS to be used for the Solution</li> <li>b) The Database Design Document outlines tasks and responsibilities for database administration and reporting, including performance monitoring, efficiency, backup and recovery.</li> <li>c) The document indicates key design decisions.</li> <li>d) The document includes a detailed database design, including data formats, data software objects, data structures, and database management</li> </ul>	<ul style="list-style-type: none"> <li>a) Logical Data Model</li> <li>b) Physical Data Model</li> <li>c) Entity Relationship Diagram (ERD) for the logical data model</li> <li>d) Data Flow Diagrams</li> </ul>	Type C	A.14

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>system files.</p> <p>e) The document describes how the preliminary data design documented in the Logical Data Model are transformed into more technical system design specifications from which the system will be built.</p>			
<b>Deliverable 24</b>	Data Dictionary	Once per release upon State approval	<p>The Data Dictionary comprehensively outlines the data element name, type, length, source, validation rules, maintenance (create, read, update, delete (CRUD) capability), data stores, outputs, aliases, and description.</p> <p>The Data Dictionary shall provide a data classification of all data collected and transferred by the Solution.</p>	<p>a) The Data Dictionary characterizes data formatting requirements and validation rules</p> <p>b) The Data Dictionary describes the data classification of database elements (entity, attributes etc.)</p>		Type C	A.14 A.19
<b>Deliverable 25</b>	SOA Models	Once per release upon State approval	<p>SOA Models will outline a services portfolio by identifying services, defining a service hierarchy, and classifying the services based on this hierarchy. This will involve defining the coarse-granularity and fine-granularity of services. This document</p>	<p>a) The SOA Models identify the Services Portfolio Management requirements, which must include the requirements for how often services should</p>	<p>a) Service Oriented Architecture (SOA) Model including but not limited to:</p> <p>b) Definition of service hierarchy</p> <p>c) Prioritization of key services</p>	Type C	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			must identify and prioritize the key services and the mechanisms to create the service layers using industry standards.	<p>be reviewed, how often they should be updated, and how they should be published</p> <p>b) The SOA Models identify the Quality of Service requirements for each service, which will involve defining scalability, availability, and response time (latency) of services in order to ensure that they are within the promised range</p> <p>c) The SOA Models identify interface requirements, which will involve both internal and external Partners and ensuring that the new System is sufficiently scalable and flexible to support the number of interfaces that will be required.</p>	<p>d) Mechanisms to create service layers</p> <p>e) Technical Architecture Diagrams</p> <p>f) Quality of Service Requirements</p> <p>g) Interface Requirements</p> <p>h) Security Requirements</p> <p>i) Performance Requirements</p> <p>j) Operational Requirements</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>Interface requirements must also include defining what communications should be asynchronous, and what communications should be synchronous</p> <p>d) The SOA Models identify security requirements, which may include encryption, authentication, data protection, and constraints on performing certain operations</p> <p>e) The SOA Models identify performance requirements, which may include the expected response time for application tasks, failover support for applications, and hours of availability</p> <p>f) The SOA Models identify</p>			

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				operational requirements, which may include server needs, scalability requirements, hosting requirements, monitoring, load balancing, failover, fault recovery, accounting and metering			
<b>Deliverable 26</b>	Functional Design Document (Including Use Cases)	Once per release upon State approval	The Functional Design Document expands upon the requirements document to describe how the functional requirements will be implemented. This document goes to a granular level and describes such things as the tables to be updated, fields to be added, screens to be created or changed, business rules to be changed, and additional interfaces.	<ul style="list-style-type: none"> <li>a) Accounts for all functional requirements</li> <li>b) Demonstrates how functional requirements will be addressed within the design</li> <li>c) Use cases that describe how the requirements will impact the system, included both positive and negative use cases.</li> <li>d) Business Process Flow Diagrams detailing the Business Process that is being introduced or enhanced.</li> </ul>	a) Systems Design Document	Type C	A.15 A.16 A.26
<b>Deliverable</b>	Technical	Once per	A Technical Design	a) Contains	a) Technical	Type C	A.15

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
27	Design Document	release upon State approval	<p>Document reflects the details required for System development/configuration and operation. This document must be developed based on outputs from the technical design sessions conducted with all Stakeholders and/or functional design, interface control documents. The Technical Design Document must include the following components:</p> <ul style="list-style-type: none"> <li>b) Detailed description of System architecture</li> <li>c) Entity Relationship Diagrams, Create, Retrieve, Update, Delete details for database elements for the component being elaborated in the design</li> <li>d) Data Flow Diagrams</li> <li>e) Processing controls</li> <li>f) Processes to manage System</li> </ul>	<ul style="list-style-type: none"> <li>a) detailed description of system architecture.</li> <li>b) Includes entity relationship diagrams and data flow diagrams</li> <li>c) References the data dictionary (i.e., all data elements are represented in the data dictionary)</li> <li>d) Specifies processing controls</li> <li>e) Specifies installation, configuration, and backup procedures</li> <li>f) Includes security controls</li> <li>g) Addresses availability and resilience controls such as load balancing, failover, and fault tolerance</li> <li>h) References ICDs</li> <li>i) Requirements and Design components mapped appropriately in</li> </ul>	<ul style="list-style-type: none"> <li>a) Architecture Diagrams</li> <li>b) Systems Design Document</li> <li>c) Business Rules</li> <li>d) Document Print/Letter/Notices/Electronic Output Management Plan</li> <li>e) Configuration Management Plan</li> <li>f) Backup Management Plan</li> <li>g) Availability and Performance Plan</li> <li>h) Interface Control Documents</li> </ul>		A.16 A.26

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>installation and configuration</p> <p>g) Data backup procedures</p> <p>h) Availability and resilience controls such as load balancing, failover capabilities, and fault tolerance.</p> <p>The Technical Design Document must include, at a minimum, the interface definitions and design (including XML/SOAP specifications for file formats), the new System design based on reviewing existing class diagrams, sequence diagrams, updated object models that represent the internal workings and designs of the containing subsystems that will expose the services, and the component specification (details of the component that will implement the service) and service assignment to each layer defined in the System architecture.</p>	configuration management database			
<b>Deliverable 28</b>	Service Level Agreements (SLAs)/Memorandum of Understandings (MOUs)	Once per release upon State approval	A Service Level Agreement(s) (SLA) is a contractual agreement between an internal or external service provider and their customer specifying performance	a) The SLA/MOU outlines the agreed upon period of performance and any performance	<p>a) Service Level Management Plan</p> <p>b) Service Level Agreements</p> <p>c) Memorandum of</p>	Type B	A.10 A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			guarantees with associated penalties should the service not be performed as contracted. A Memorandum(s) of Understanding (MOU) is a legal document that outlines the terms and details of an agreement between parties, including of each party's requirements and responsibilities.	<p>guarantees with associated complications falling within the period as well as reporting mechanisms/frequency and review process.</p> <p>b) The SLA/MOU includes a process to be followed in the event that an agreement change is to be made</p> <p>c) The SLA/MOU escalation process is included and detailed in nature</p>	Understanding		
<b>Deliverable 29</b>	Automated Code Review Results	Once per release upon State approval	This deliverable will display the results from an automated tool's code review. These results will be used by developers to address issues in the coding. This will also be helpful in determining the overall quality of the code being produced.	<p>a) Results are comprehensive of code.</p> <p>b) Results provide evidence to indicate product quality.</p> <p>c) Results indicate level of compliance with coding standards.</p>	a) Coding Standards and Quality Review Plan	Type A	A.10
<b>Deliverable 30</b>	System Configuration Document	Once per release upon State approval	A System Configuration Document captures all the configuration information of the systems. This document	<p>a) Documents all system configuration elements (software,</p>	<p>a) Configuration Management Plan</p> <p>b) Asset Management</p>	Type C	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			often contains: Network configuration by interface, disk partition layout, installed software, with any significant configuration information, hardware and peripherals inventory, physical location of system, authentication information, network integration information (e.g., Network Time Protocol (NTP) configuration, Domain Name System (DNS) resolver configuration), list of authorized super users, list of authorized pseudo users, list of individual(s) responsible for system, with contact information (preferably via multiple communication channels), OS version information, installation idiosyncrasies and patches installed. With good system configuration documentation, a system can be rebuilt from scratch, as well as it can handle other disaster recovery tasks.	<p>hardware, OS, network configuration, authentication)</p> <p>b) Information can be validated to be accurate and current (e.g., release and patch levels reflect current installation)</p> <p>c) Reflects all approved configuration changes (managed through Technical Change Control Board)</p>	Plan		
<b>Deliverable 31</b>	Unit, System, Regression, and Integration Test Scripts	Once per release upon State approval	This deliverable documents the configuration decisions made in developing the Solution, and includes	<p>a) Tests are traceable to requirements.</p> <p>b) Tests have been reviewed for</p>		Type C	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>traceability of configuration decisions to requirements and design. It includes information such as network configuration by interface; disk partition layout; installed software, with any significant configuration information – hardware and peripherals inventory; physical location information; authentication information (method used, configurations for method, etc.); network integration information (e.g., NTP configuration, DNS resolver configuration); list of authorized superusers; list of individual(s) responsible for system, with contact information (preferably via multiple communication channels); OS version information and installation idiosyncrasies; patches installed. This documentation is critical to support staff in operations and maintenance, and also supports disaster recovery tasks as well as OS patch maintenance.</p>	<p>relevance to the respective requirement.</p> <p>c) Tests have been defined for unit, system, regression and integration testing that provide complete coverage to all testable requirements</p> <p>d) Section 508 testing package</p>			
<b>Deliverable</b>	Unit, System,	Once per	Test scripts provide	a) Test activities	a) Test Reports	Type A	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
32	Regression, and Integration Testing Test Results	release upon State approval	instructions (written using a scripting/programming language) to be performed on a system under test to verify that the system performs as expected. Unit tests occur on individual functions; system integration tests validate performance of multiple sub-systems within the Solution.	<p>and results are documented by module.</p> <p>b) Defects and retest results are documented.</p> <p>c) Test results demonstrate completion of all required tests and testing against all requirements.</p>	<p>and summary reports for unit, system, Regression, integration testing for all areas being tested</p> <p>b) Section 508 Assessment Package results</p> <p>c) Test Summary Report</p>		
<b>Deliverable 33</b>	System Readiness Certification for UAT	Once per release upon State approval	This deliverable documents completion of testing and associated results for testing completed by the system integrator. Results should indicate success rate, defects, retest results, and completion percentage of tests vs. requirements.	<p>a) Open defects have been determined by State to be low impact and low risk.</p> <p>b) All functional and non-functional requirements have been delivered unless change requests have provided for de-scoping or deferral.</p> <p>c) Modules and components demonstrated stable performance during SIT and performance and capacity testing.</p> <p>d) Release notes have been</p>	<p>a) Test Reports</p> <p>b) Section 508 Assessment Package results</p> <p>c) Test Summary Report</p>	Type A	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				developed to document functionality included in release.			
<b>Deliverable 34</b>	Formal Acceptance Testing Report (successful completion of UAT) -Performance Test Results -System Runbook and Troubleshooting Guide -System and Operational Readiness Checklist -Data Conversion Report	Once per release upon State approval	The Formal Acceptance Testing report documents completion of UAT and final steps prior to implementation into production. This report includes documentation to support use and maintenance of the Solution, as well as evidence that readiness activities – including transition requirements – have been completed.	<ul style="list-style-type: none"> <li>a) UAT results are documented, and demonstrate no defects beyond low impact or low risk.</li> <li>b) Troubleshooting guide has been validated by user and support staff for accuracy and relevance of topics.</li> <li>c) Data conversion has been completed successfully; any exceptions have been determined by HCFA to be low impact or low risk.</li> <li>d) All checklist activities for operational readiness have been completed.</li> <li>e) Release notes have been developed to document functionality</li> </ul>		Type A	A.10

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				included in release.			
<b>Deliverable 35</b>	Contingency/ Recovery Plan	All CPs will be reviewed and exercised annually.	<p>The Contingency/Recovery Plan establishes procedures to recover a system following a disruption. The Contingency/Recovery Plan. The Plan identifies the activities, resources, and procedures needed to carry out operations during prolonged interruptions to normal operations. The Plan also assigns responsibilities to designated personnel and provides guidance for recovering the system. CP Test Plan should be tested to identify and rectify deficiencies and planning shortfalls, NOT to ascertain the technical competence of personnel with recovery responsibilities. The Business Owner, System Developer/Maintainer, Contingency Plan Coordinator, and SSO shall establish criteria and pre-developed test plan for validating/test CPs on an annual schedule, once every 365 days. CP Test After Action Report will be used for plan updates addressing</p>	<p>a) The Contingency/Recovery Plan defines the triggers that would initiate the contingency and recovery operations</p> <p>b) The Contingency/Recovery Plan outlines the individuals with the responsibility/authority to make the decision to initiate the Contingency/Recovery Plan</p> <p>c) The Contingency/Recovery Plan clearly outlines the steps and activities to be taken in the event of a trigger.</p> <p>d) The Contingency/Recovery Plan outlines a dry run simulation of the contingency activities.</p> <p>e) The</p>	<p>a) Disaster Recovery Plan</p> <p>b) Disaster Recovery Plan Test</p> <p>c) Business Continuity Plan</p> <p>d) Asset Management Plan</p> <p>e) Configuration Management Plan</p> <p>f) Business Continuity Test Plan</p> <p>g) Configuration Management Database</p> <p>h) Build Books for STS</p>	Type A	A.14

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			any identified shortcomings.	<p>Contingency/Recovery Plan outlines the communication protocols and flows in the event the Contingency/Recovery Plan is evoked.</p> <p>f) The Contingency/Recovery Plan should include an approach to test the contingency plans.</p> <p>g) Contingency/Recovery Test After Action Report must be clearly defined.</p>			
<b>Deliverable 36</b>	Beta Test Plan	Once per release upon State approval	A Beta Test Plan is a test plan that is used to describe the methodologies, processes, and testing that is expected to take place on a beta release (non-production release of full functionality).	<p>a) The plan outlines methodologies and processes to be used.</p> <p>b) The plan outlines specific testing activities to be performed, including expected outcomes.</p> <p>c) The plan outlines the individuals who will be involved in beta testing</p>		Type A	A.16

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				and the process for documenting identified issues.			
<b>Deliverable 37</b>	Network Vulnerability Assessment Resolution Report	Once per release upon State approval	The Network Vulnerability Assessment Resolution Report outlines results of a network vulnerability assessment, the significance of findings, and the completed and planned actions to resolve identified vulnerabilities.	<ul style="list-style-type: none"> <li>a) The Network Vulnerability Assessment Resolution Report includes a status on all open items identified in the assessment.</li> <li>b) The Network Vulnerability Assessment Resolution Report defines the anticipated approach and timeline for resolving open issues based on criticality and severity.</li> <li>c) The Network Vulnerability Assessment Resolution Report indicates progress in resolving issues that were identified in previous assessments.</li> </ul>	a) Software Assurance Misuse Cases	Type B	A.10 A.19
<b>Deliverable 38</b>	Beta Test Evaluation Report	Once per release upon State approval	A Beta Test Evaluation Report is a report that details the results of a Beta test release. The report will:	<ul style="list-style-type: none"> <li>a) The beta test report details the test environment (number of testers, types of machines used)</li> </ul>		Type A	A.16

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<ul style="list-style-type: none"> <li>a) Compare actual results to expected results</li> <li>b) Identify major defects found with mitigation plans</li> <li>c) Capture feedback and pain points reported by the users testing the system</li> </ul>	<ul style="list-style-type: none"> <li>that was used to execute the beta test</li> <li>b) The beta test details the key functionality that was tested</li> <li>c) The beta test compares actual test results with expected testing results</li> <li>d) Any new risks, issues, and defects found during testing have been properly identified, documented, and prioritized</li> </ul>			
<b>Deliverable 39</b>	Privacy Impact Assessment	Reviewed annually or upon significant system change	Required of federally owned systems. The Privacy Impact Assessment (PIA) is designed to help states quickly identify and subsequently document the specific types of sensitive information that it will collect, process, and store. The Privacy Impact Assessment (PIAs) identifies systems that contain personally identifiable information (PII) and satisfies system compliance with all relevant privacy laws, regulations, and guidance. The PIA	<ul style="list-style-type: none"> <li>a) The PIA approved by the HCFA Chief Privacy Officer</li> <li>b) The PIA is sufficient enough to be used to obtain an Authority to Operate (ATO) subject to review/approval by CMS</li> </ul>		Type B	A.10 A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			document ensures that privacy protections are incorporated into every stage of an IT system's life cycle, and measures the effectiveness of these protections.				
<b>Deliverable 40</b>	Information Security Risk Assessment	As defined by CMS	<p>Required of federally owned systems. The IS RA contains a list of threats and vulnerabilities, an evaluation of current security controls, their resulting risk levels, and any recommended safeguards to reduce risk exposure. The IS RA also supports risk management through the evaluation of risk impact upon the enterprise security model. It will be used for system certification and accreditation (C&amp;A). CMS requires each Business Owner to develop or update an IS RA in response to each of the following events:</p> <ul style="list-style-type: none"> <li>a) New system;</li> <li>b) Major business process or technology/system modification(s);</li> <li>c) Every third year of an operational system;</li> </ul>	<ul style="list-style-type: none"> <li>a) The IS RA contains a list of threats and vulnerabilities to the system</li> <li>b) The IS RA provides the results of an evaluation of current security controls and their resulting risk levels</li> <li>c) The IS RA includes any recommended safeguards in an attempt to reduce risk exposure.</li> <li>d) The IS RA approved by the HCFA Chief Privacy Officer</li> <li>e) The IS RA is sufficient enough to be used to obtain an ATO subject to review/approval by CMS and required for</li> </ul>	<ul style="list-style-type: none"> <li>a) Information System Risk Assessment</li> <li>b) Information Security Risk Assessment</li> </ul>	Type B	A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<ul style="list-style-type: none"> <li>d) Increase in security risks/exposure;</li> <li>e) Increase of overall system security level; and/or,</li> <li>f) Serious security violation(s) as described in the CMS</li> <li>g) Information Security Incident</li> <li>h) Handling and Breach Analysis/Notification Procedure</li> </ul>	Authority to Connect (ATC)			
<b>Deliverable 41</b>	Data Use/Data Exchange/Interconnection Security Agreements	Once per release upon State approval	Information that is required to develop agreements between parties for the use of personal identifiable data, and to ensure secure data exchange. This includes information that the IRS Office of Safeguards expects from an agency regarding their procedures for safeguarding Federal Tax Information (FTI), in any instance where that agency intends to receive, store, process, or transmit FTI.	<ul style="list-style-type: none"> <li>a) The document clearly delineates the roles and responsibilities between parties that are exchanging data</li> <li>b) The document sufficiently addresses the mechanisms for data exchange</li> <li>c) The document sufficiently addresses security controls in place by each party of the agreement, and how those controls will be used together to</li> </ul>		Type B	A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>ensure a secure exchange of data</p> <p>d) The document has been signed by resources who have the proper authority to enter the organization into such agreement</p>			
<b>Deliverable 42</b>	MARS-E Security Controls	System Security Plan should be reviewed and updated on an as needed basis, including annually, and when there are major system modifications that could potentially impact the security and privacy of the information system.	The MARS-E Security Controls Document provides guidance to CMS and its contractors as to the minimum level of required security controls that must be implemented to protect CMS' information and information systems.	<p>a) The MARS-E Security Controls Document is compliant with the Minimum Acceptable Risks for Exchanges document</p> <p>b) Assessment of MARS-E compliance shall be done using NIST Publication SP 800-53A "Guide for Assessing the Security Controls in Federal Information Systems and Organizations" standards</p> <p>c) The document can be used to secure an ATO</p> <p>d) The document is</p>	<p>a) SSP Workbook (Security Control Description)</p> <p>b) Business Risk Assessment (Security Awareness) Training Plan</p> <p>c) (Security Awareness) Training Result</p> <p>d) Computer Matching Agreement (CMA)</p>	Type A	A.17 A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				signed by the HCFA Chief Security Officer			
<b>Deliverable 43</b>	IRS Safeguards Procedures Report	The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security authorization . All information regarding the authorization shall be provided to the Office of Safeguards as part of the Safeguard Activity Report.	Supports HCFA in attaining IRS certification for the Solution. Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must have an approved SSR prior to having access to FTI. Section 7 of Publication 1075 outlines SSR Reporting Requirements — 6103(p) (4) (E): <ul style="list-style-type: none"> <li>a) The agency should submit the report for approval at least 90 days prior to the agency receiving FTI.</li> <li>b) The agency must update and submit the SSR annually to encompass any changes that impact the protection of FTI.</li> <li>c) The SSR submission and all associated attachments must be sent annually to identify changes to safeguarding</li> </ul>	<ul style="list-style-type: none"> <li>a) The document is completed in time enough to provide the IRS the 90-day period needed before accessing FTI</li> <li>b) The document is completed using the IRS SSR prescribed template</li> <li>c) The document is approved by the HCFA CFO prior to submission to the IRS subject to review/approval by CMS/IRS and required for ATC</li> </ul>		Type B	A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			procedures.				
<b>Deliverable 44</b>	Site Readiness Reports	Once per release upon State approval	The Site Readiness Reports are based on the results of the site assessments and will address all remote sites in the State. Each Site Readiness Report will detail issues at each particular site and make recommendations on how each issue will be remedied before the rollout of the new System.	<ul style="list-style-type: none"> <li>a) The Site Readiness Report addresses all of the readiness criteria</li> <li>b) The Site Readiness Report identifies deficiencies, remediation, and a recommendation on whether or when to proceed with implementation.</li> </ul>		Type A	A.23
<b>Deliverable 45</b>	System Operations Documentation	Once per release upon State approval	<p>The System Operations Documentation describes all required Systems operational activities and must encompass System functionality from a remote user's perspective, a State business user's perspective, and from an information technology and System operations perspective. These manuals must include:</p> <ul style="list-style-type: none"> <li>a) A description of how to use the System based on user roles and responsibilities</li> <li>b) A list of prebuilt reports and their</li> </ul>	<ul style="list-style-type: none"> <li>a) The document addresses all areas of system operation, as prescribed in the description</li> <li>b) The document has been approved by the appropriate HCFA resources</li> </ul>	<ul style="list-style-type: none"> <li>a) User Manuals</li> <li>b) Release Notes</li> </ul>	Type A	A.15

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>descriptions</p> <p>c) A description of all screens and how they are interrelated, and all help and navigation functions and how to use them</p> <p>d) A complete list of error messages, their descriptions, and how to resolve the errors</p> <p>e) A list of all included System documentation and its use</p> <p>f) How to troubleshoot common System problems</p> <p>g) A description of the key data tables, elements, and their contents</p> <p>h) How to perform System maintenance functions like data backup and recovery, run batch processes (if applicable), perform data cleanup, and administer user</p>				

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			accounts and permissions i) How to troubleshoot common System problems j) A listing of all logs and how to interpret them k) Key System capacity and security management considerations l) Contact information for receiving support m) Where to find disaster recovery and business continuity information related to the System n) A listing of System interfaces and how to troubleshoot communications problems o) File descriptions p) System and System environment configuration baseline				
<b>Deliverable</b>	System	Once per	The System	a) The System	a) O&M Manual	Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
46	Maintenance, Support and System Transition Plan	release upon State approval	Maintenance, Support and System Transition Plan must outline the transition of system Operations and Maintenance from the Vendor to the State's hosting model. The Plan should note all procedural, staffing, and resource requirements.	<p>Maintenance, Support and System Transition Plan will indicate the amount of dedicated resources providing O&amp;M support, and how sufficient resources will be provided while in support of development activities for future releases.</p> <p>b) The System Maintenance, Support and System Transition Plan will identify all procedures and activities to be transitioned to O&amp;M.</p>	b) Service Transition Plan		A.18
<b>Deliverable 47</b>	Infrastructure, System Source Code and Documentation	Once per release upon State approval	This is the delivery to the State of written custom code, solutions, and documentation that a Contractor has bought or developed. Once the state has approved the Solution by way of successful testing and Gate Reviews, the Solution becomes State property.	a) The Solution has successfully made it through the formalized Gate Review process and testing and accepted by the state as an approved Solution	<p>a) Business Product</p> <p>b) Configuration Management Plan</p> <p>c) Configuration Management Database</p> <p>d) Data Dictionary</p>	Type A	A.18
<b>Deliverable 48</b>	Updated System	Once per release	This is updated code, Solution, or	a) The Solution has successfully		Type A	A.18

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
	Source Code and Design Documentation	upon State approval	documentation that the Contractor has updated from a prior release. Once the state has approved the changes to the Solution by way of successful testing and Gate Reviews, the Solution becomes State property.	made it through the formalized Gate Review process and testing and accepted by the state as an approved Solution			
<b>Deliverable 49</b>	Infrastructure Services Deployment Report	Once per release upon State approval	<p>The Infrastructure Services Deployment report must address the implementation of the following infrastructure services related to the System:</p> <ul style="list-style-type: none"> <li>a) Remote Access Infrastructure</li> <li>b) Patch and Remote Security Management Infrastructure</li> <li>c) Service Desk Enhancements</li> <li>d) Code Migration Infrastructure</li> <li>e) Software Configuration Management Infrastructure</li> <li>f) Change and Release Management</li> <li>g) Data Retention and Archiving Infrastructure</li> <li>h) Performance Reporting Infrastructure</li> </ul>	a) The report includes the prescribed sections as described in the description	a) Infrastructure Services Deployment	Type A	A.10 A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
<b>Deliverable 50</b>	Plan of Action and Milestones (POA&M)	Review and update Monthly and submit to CMS quarterly	The Plan of Action and Milestones (POA&M) is a management process that outlines weaknesses and delineates the tasks, timeline and completion criteria necessary to mitigate them.	<ul style="list-style-type: none"> <li>a) The POA&amp;M contains findings from internal and external audits, as well as issues that surfaced as part of the certification process</li> <li>b) All POA&amp;Ms need to have a Corrective Action Plan which includes a root cause analysis, mitigation alternatives and risks associated with each, and strategies for preventing recurrence</li> </ul>	<ul style="list-style-type: none"> <li>a) POA&amp;M Management Plan</li> </ul>	Type A	A.19
<b>Deliverable 51</b>	Interconnected Systems Agreement (ISA)	ISAs need not be reissued unless a significant system change has occurred or three years have elapsed since issuance.	Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and the State. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same Authorizing Official. The ISA documents the security protections that must operate on	<ul style="list-style-type: none"> <li>a) The ISA addresses the development, management, operation, and security of a connection between CMS and the State.</li> <li>b) The ISA contains a description of the information and data that will be made available, exchanged, or passed one-way</li> </ul>	<ul style="list-style-type: none"> <li>a) Security Control Assessment Report</li> <li>b) ATO Submission</li> <li>c) CMS CTO-issued ATO</li> </ul>	Type A	A.19

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			interconnected systems to ensure that transmission between systems permits only acceptable transactions. An ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. An ISA must be reissued whenever a significant change occurs to any of the interconnected systems.	<p>only by the interconnection of the two systems/networks.</p> <p>c) The ISA describes and documents the information handled by the system and the overall system security level as LOW, MODERATE or HIGH</p> <p>d) The ISA contains a topological drawing that illustrates the interconnectivity between both systems, including all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Subject to review/approval by CMS and required for ATC</p>			
<b>Deliverable 52</b>	SLA, System Performance, System QA	Weekly and Monthly, based on	These reports measure the systems adherence to the prescribed SLAs,	a) The report provides metrics to show the		Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
	Reports	type of SLA	tracks current system performance, and system quality.	<p>systems performance in reference to prescribed SLAs</p> <p>b) The report provides metrics to show the overall performance of the system</p> <p>c) The report includes metrics that demonstrates open defects, priority of defects, and the rate at which defects are being resolved</p>			
<b>Deliverable 53</b>	System Incident and Corrective Maintenance Reports	Monthly	The System Incident and Corrective Maintenance Report will outline corrective maintenance requests identified throughout the duration of the Warranty period. Each maintenance request will have a description, resolution status, and course of action for remedying all open maintenance requests.	<p>a) The System Incident and Corrective Maintenance Report will include anticipated resolution times for all open corrective maintenance requests as well as root cause and number of impacted cases and/or members.</p> <p>b) The System Incident and Corrective Maintenance</p>		Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				<p>Report will link defects to the release for warranty tracking purposes.</p> <p>c) The System Incident and Corrective Maintenance Report includes ageing, criticality and severity, and an analysis approach to defect reporting.</p>			
<b>Deliverable 54</b>	Operations Report	Daily (Calendar Days) and Monthly	<p>The Daily and Monthly Operation Reports shall include:</p> <ul style="list-style-type: none"> <li>a) Interface events/issues</li> <li>b) System event/issues</li> <li>c) Software event/issues</li> <li>d) Errors and Anomalies</li> <li>e) Transactions Sent and Received (Daily, Total Amount)</li> <li>f) Transaction Types</li> <li>g) Staffing/Operational Activities and Issues</li> <li>h) Number of notices/letters received and</li> </ul>	<p>a) The reports contain all of the required elements as agreed upon by HCFA and the Contractor.</p>	<p>a) Security Monitoring Reports</p>	Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>sent (including any/all reconciliation efforts)</p> <ul style="list-style-type: none"> <li>i) Cumulative statistics and complete breakdown of all letters and notices by type</li> <li>j) Performance against SLA</li> <li>k) Average response times (for SLA validation)</li> </ul>				
<b>Deliverable 55</b>	AOA Report	Annual	<p>The AOA Report evaluates investment operational results against investment objectives.</p> <p>The AOA Report should include the following sections:</p> <ul style="list-style-type: none"> <li>a) Overview</li> <li>b) Cost Benefit Analysis</li> <li>c) Schedule Analysis</li> <li>d) Performance Analysis</li> <li>e) Risk Analysis</li> <li>f) Improvement</li> <li>g) Recommendations and Approvals</li> </ul>	<ul style="list-style-type: none"> <li>a) The document provides an overview of the current operation of the system and how it fits within the organization's investment objectives.</li> <li>b) The document includes all sections as prescribed in the document description</li> <li>c) The document has the necessary signatures</li> </ul>		Type A	A.10
<b>Deliverable 56</b>	Warranty Completion Report	Monthly until completion of warranty	Report validates that the hardware, customized IMS, and supporting	<ul style="list-style-type: none"> <li>a) The report is produced while the Solution is</li> </ul>	<ul style="list-style-type: none"> <li>a) Project Completion Report</li> </ul>	Type A	A.26

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			software are performing in a stable manner. Report summarizes the current state of production including open issues, transition status and production environment performance statistics.	<ul style="list-style-type: none"> <li>b) This report is sufficient enough to communicate needed fixes covered under the warranty</li> </ul>	<ul style="list-style-type: none"> <li>b) Project Closeout Report</li> <li>c) Disposition Plan</li> </ul>		
<b>Deliverable 57</b>	Post Implementation Report	Once per release upon State approval	This Post Implementation Report results from monitoring the performance of the system/application during normal operations against original user requirements and any newly implemented requirements or changes.	<ul style="list-style-type: none"> <li>a) The Post Implementation Report contains steps to gather and take action on lessons learned on activities executed in all Solution releases.</li> <li>b) The Post Implementation Report contains a User/Customer Assessment based on feedback received</li> <li>c) The Post Implementation Report contains a Performance Assessment</li> <li>d) The Post Implementation Report contains justification as to if the existing system should</li> </ul>		Type A	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				continue in operation as is, be enhanced, or terminated. If the system is to be enhanced or terminated, summarize the actions to be taken this fiscal year.			
<b>Deliverable 58</b>	O&M Runbook	Monthly	The O&M Runbook contains information and strategies designed to guide operational stakeholders in the normal use and maintenance of the Solution. The manual should be designed in a manner that facilitates actions and responses to anything that may arise during normal product operations and maintenance including but not limited to incident, problem, request, asset, event, and IT change management activities. The O&M Runbook guides those who maintain, support and/or use the system in a day-to-day operations environment.	<ul style="list-style-type: none"> <li>a) The O&amp;M Runbook incorporates testing, training, and reinforcement exercises that are planned and implemented.</li> <li>b) The clarity and effectiveness of the O&amp;M Runbook has been validated through sample testing by representative users.</li> <li>c) The O&amp;M Runbook defines the target audience for specifies sections of the Runbook.</li> <li>d) The O&amp;M Runbook defines the necessary skills required to perform said</li> </ul>	<ul style="list-style-type: none"> <li>a) Technology Change Management Plan</li> <li>b) Configuration Management Plan and Database</li> <li>c) Assets Management Plan</li> <li>d) Event Management Plan</li> <li>e) Incident Management Plan</li> <li>f) Problem Management Plan</li> <li>g) Request Management Plan</li> </ul>	Type C	A.17

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
				activities.			
<b>Deliverable 59</b>	System Go-Live Report	Once per release upon State approval	The System Go-Live Report is a record of how the implementation went. The focus is on deviations from what was considered default or what was planned. This information is critical for a successful transition to maintenance. It is also useful for project closure and for archival for future projects.	<ul style="list-style-type: none"> <li>a) Describes at a high level the major problems encountered during data conversion activities and corrective actions that were applied to solve them</li> <li>b) Describes at a high level the major problems encountered while establishing the Production Environment and corrective actions that were applied to solve them</li> <li>c) Describe at a high level the major problems encountered during the move of the application to the production environment and corrective actions that were applied to solve them</li> </ul>		Type B	A.17
<b>Deliverable 60</b>	Operational Readiness Plan and Report	Once per release upon State approval	The Operational Readiness Plan and Report details and reports how the	<ul style="list-style-type: none"> <li>a) The Operational Support Plan been completed and signed off.</li> </ul>	<ul style="list-style-type: none"> <li>a) Operational Readiness Plan and Report</li> </ul>	Type A	A.15

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle	Contract Section Reference
			<p>system/application is put into Production without verification that it meets performance requirements and that the operation and maintenance procedures ensure prompt system recovery without loss of data.</p> <p>The Operational readiness plan provides a checklist and an approach for carrying out readiness assessments activities.</p> <p>The Operational readiness activities include a review of the integrity of system data (data cleansing) and readiness for data conversion.</p> <p>The Operational readiness plan provides a mechanism to identify areas of deficiencies with sufficient detail to allow the business unit to prepare an action plan in response to the deficiency.</p> <p>The Operational readiness plan defines a communication plan which identifies points of contact for the relevant implementation stakeholders.</p>	<ul style="list-style-type: none"> <li>b) The Plan should ensure that the transition and knowledge transfer has successfully been completed and/or a O&amp;M Contractor is in place</li> <li>c) The technical policies and processes are successfully operated in production</li> <li>d) User IDs for all roles are setup</li> </ul>	<ul style="list-style-type: none"> <li>b) System of Record Notice</li> <li>c) Operational Readiness Checklist</li> </ul>		

## A.28 Change Order – Special Projects & Enhancement

- A.28.1 Special Projects are additional projects that the State may, at its sole discretion, initiate and assign to the Contractor during the DDI phase of the Contract for the performance of services, fulfillment of additional requirements, or creation of deliverables (Services) outside those set forth in the DDI Scope of Services of this Contract. Special Projects shall be funded from the Change Order Fund that is a maximum of fifteen percent (15%) of the total Contract liability described in Section C.3 of this Contract.
- A.28.2 All Special Projects shall be associated with a Gate Review as determined by the State and not paid until approved as part of the Gate Review process.
- A.28.3 Enhancements are additional projects that the State may, at its sole discretion, initiate and assign to the Contractor during the O&M phase of the Contract for the performance of Services outside those set forth in the O&M Scope of Services of this Contract (See Section A.10.13.5). Enhancements shall be funded from the Enhancements Fund that is a maximum of ten percent (10%) of the total Contract liability described in Section C.3.
- A.28.4 Change Orders shall be implemented by a Control Memorandum as described in Section A.29.
- A.28.5 Change Order Creation – After receipt of a written request for the performance of Services, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the Services. Contractor’s proposal must specify:
- A.28.5.1 the effect, if any, of implementing the requested change(s) on all other services required under this Contract;
  - A.28.5.2 a description of the units of service needed to complete the Change Order;
  - A.28.5.3 the specific effort involved in completing the change(s);
  - A.28.5.4 the expected schedule for completing the change(s);
  - A.28.5.5 the maximum number of person hours required for the change(s); and
  - A.28.5.6 a fixed price for all Services under the Change Order based on the Contractor’s rate card as detailed in this Contract. The maximum cost for the Services shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.
- A.28.6 The Contractor shall not perform any Services under the Change Order until the State has approved the Change Order proposal. If approved, the State will sign the proposal, and it shall constitute a binding agreement between the Parties pertaining to the specified change(s) and shall, under this provision, be incorporated into this Contract by reference. All terms of this Contract, including but not limited to Warranty and Liquidated Damages shall apply to services provided under Change Orders.
- A.28.7 Change Order Performance— Subsequent to creation of a Change Order, the Contractor shall complete the required Services. The State shall be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.

A.28.8 Change Order Remuneration— The State will remunerate the Contractor only for work the State deems acceptable. All acceptable work performed pursuant to an approved Change Order shall be remunerated in accordance with Contract Section C.3.c, PROVIDED THAT, the State shall be liable to the Contractor only for the cost of the actual goods or services provided to complete the necessary work, not to exceed the maximum cost for the change detailed in the Change Order. In no instance shall the State be liable to the Contractor for any amount exceeding the maximum cost specified by the Change Order authorizing the goods or services. Upon State approval of the work, the Contractor shall invoice the State in accordance with the relevant provisions of this Contract.

#### A.29 Control Memorandum Process

A.29.1 The Control Memorandum (“CM”) process shall be utilized by the State to clarify Contract requirements, issue instruction to the Contractor, document action required of the Contractor, or request information from the Contractor. In addition, the CM process shall be used by the State to impose assessments of damages, either actual or liquidated. This process will be used to address issues or matters that do not require a contract amendment. Each CM must be in writing and indicate the date on which it was issued. CMs may provide relevant history, background, and other pertinent information regarding the issue(s) being addressed in the CM. Each CM will establish a deadline or timeframe for the Contractor’s reply or other action. All CMs submitted to the Contractor must be signed and approved by the State’s Project Director (or his/her designee). When the CM pertains to damages, either actual or liquidated, the State may issue consecutive CMs, as may be necessary or appropriate.

- A.29.1.1 A CM may include one (1) or more of the following five (5) components of the CM process described below:
- a) On Request Report – a request directing the Contractor to provide information by the time and date set out in the CM.
  - b) Control Directive (CD) – instructions that require the Contractor to complete, within a designated timeframe, one (1) or more deliverables or to perform any other request from the State that is within the scope of the Contract. A CD may also provide clarification of certain Contract terms. Once a CM/CD has been issued, it shall be considered to be incorporated into this Contract.
  - c) Notice of Potential Damages (Actual or Liquidated) (NPD) – notification to the Contractor that the State has determined that a potential Contract performance or compliance issue exists and that the State is contemplating assessing damages, actual and/or liquidated. The NPD shall identify the Contract provision(s) on which the State determination rests.
  - d) Notice of Calculation of Potential Damages (Actual or Liquidated) (NCPD) – notification to the Contractor that provides a calculation of the amount of potential damages, actual and/or liquidated, that the State is contemplating assessing against the Contractor. NPDs and NCPDs may be issued consecutively or simultaneously.
  - e) Notice of Intent to Assess Damages (Actual or Liquidated) (NIAD) – notification to the Contractor that the State is assessing damages and specifying whether the damages are actual damages, Liquidated Damages, or both, and setting out the performance or compliance issue underlying each intended damage assessment. The NIAD shall identify the NPD and NCPD upon which it is based. The NIAD shall specify the total amount and type of damages, whether actual or liquidated, the State intends to assess. Following the issuance of an NIAD, the State may elect to

withhold damages from payments due to Contractor. The State may not issue a NIAD without first issuing a NPD and a NPCD. The State may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

- A.29.2 Damages for failure to comply with CM. The Contractor shall fully comply with all CMs. Failure to do so may result in the State pursuing recovery of damages, as defined in Section E.10, including Liquidated Damages as listed in Contract Attachment 2, a corrective action plan, and/or termination of the Contract.
- A.29.3 Appeal of Damages by Contractor. Contractor may appeal either the basis for NPD or calculation of NPCD potential damages, either actual or liquidated. To do so, the Contractor shall submit to the State's Project Director (or his/her designee) a written response to the NPD and/or NPCD within ten (10) business days of receipt of a CM which includes a NPD or a NPCD. The State's Project Director (or his/her designee) shall review the appeal and provide notice of his/her determination to the Contractor through a CM. If the Contractor disagrees with the State's Project Director's (or his/her designee) initial appeal determination or the State's Project Director (or his/her designee) is unable to resolve the appeal, the Contractor may submit a written request to the State's Project Director (or his/her designee) that the matter be escalated to senior management of the Agency. Contractor shall submit such a request for escalation within ten (10) business days of its receipt of the initial appeal determination from the State's Project Director (or his/her designee) or of notification by the State's Project Director that he/she is unable to resolve the appeal. The State's senior management shall provide written notice of its final determination to the Contractor within (10) days of the receipt of the appeal from the Contractor. Upon appeal or escalation, the State shall not increase the amount of the potential damages.

### A.30 Payment

- A.30.1 The standard method for payment under this Contract to Contractor is that payment shall be as outlined in Section C upon State certification of a successful unconditional pass of the Gate Review (as described in Section C.3 below) and State approval of all deliverables associated with that Gate Review. Upon completion of both requirements, the State shall pay of 80% of the funds allocated to that Gate Review. 20% of the total monies due upon Gate Review approval will be withheld and disbursed as follows:
- A.30.1.1 Fifty percent (50%) of the amount withheld upon the next Successful Release
- A.30.1.2 Fifty percent (50%) of the amount withheld upon completion of the release's Warranty Period.
- A.30.2 Special Project Change Orders and shall be paid only upon the successful unconditional pass of the associated Gate Review and State acceptance of all associated deliverables.
- A.30.3 Enhancement Change Orders shall only be paid upon Successful Release of the Enhancement functionality.
- A.30.4 The State shall not make payments for any deliverables, regardless of their approval status, until State certification of successful unconditional pass of their related Gate Review.
- A.30.5 In the event that a Change Order necessitates changes to a deliverable approved in a previous Gate Review, the State shall consider these revised deliverables to be required

deliverables associated with the next Gate Review or subject to State approval prior to enhancement release.

- A.30.6 Following the unconditional pass of the Post Implementation Review Gate, the Contractor shall begin monthly O&M reporting and the Contractor shall invoice the monthly O&M cost as described in Section C.3.
- A.30.7 In exceptional circumstances and solely on its own initiative and in the exercise of its own discretion, the State may alter the payment and withhold structure, set forth in Section A.30.1, under this Contract. Such alterations shall be governed by the Control Memorandum process and may include:
- A.30.7.1 The State may pay Contractor an amount in excess of the amount due at the time of a successful Gate Review, if the Contractor has completed a functionality or functionalities scheduled to be included in a later Gate Review. Any such excess amount will be deducted from the amount due to the Contractor upon the successful Gate Review that was originally intended to include that functionality or functionalities.
- A.30.7.2 The State may alter the amount of the withhold, set out in Section A.30.1 by reducing the withhold amount or eliminating the withhold amount from any particular Gate Review Payment.
- A.30.7.3 The State may reallocate certain amounts due under this Contract in order to compensate Contractor for completion of duties, tasks, or intermediate deliverables, either those unspecified as described in Section A.3 that are necessary to achieve success on this Contract or those specified in the Contract.
- A.30.8 In no event shall any alteration set out above:
- A.30.8.1 increase the total amount due to the Contractor from the State under this Contract;
- A.30.8.2 result in a delay or reduction of any payment to the Contractor, except to the extent that funds have previously been paid to the Contractor as a result of an alteration; or
- A.30.8.3 be used to compensate the Contractor for any work which has not been completed at the time that the alteration of the payment or withhold structure is made.
- A.30.9 The alteration to the payment and withhold structure shall be deemed to be made at the time that the State notifies the Contractor in writing that a decision to make such an alteration has been made.
- A.30.10 The Contractor agrees and understands that the determination by the State that exceptional circumstance(s) exist (or do not exist) and the determination of the type, amount and timing of any alteration, if any, is the sole prerogative of the State and is not subject to any review.
- A.31. Nondiscrimination Compliance Requirements. The Contractor shall comply with all applicable federal and state civil rights laws, regulations, rules, and policies and Contract Section D.9 of this Contract.
- a) On an annual basis, the Contractor's staff and subcontractors assigned to perform

duties under the terms of this Contract shall receive nondiscrimination training. The Contractor shall be able to show documented proof that the training was made available to the Contractor's staff and to its subcontractors that are considered to be performing duties under this contract.

- b) The Contractor shall keep such records as may be necessary in order to submit timely, complete and accurate compliance reports that may be requested by HHS, U.S. Department of Justice ("DOJ"), HCFA, or their designees. If requested, the information shall be provided in a format and timeframe specified by HHS, DOJ, HCFA. The requested information may be necessary to enable HHS, HCFA to ascertain whether the Contractor is complying with the applicable civil rights laws.
  - c) The Contractor shall permit access as set forth in the applicable civil rights laws to HHS, DOJ, HCFA, or their designees during normal business hours to such of its books, records, accounts, and other sources of information, and its facilities as may be pertinent to ascertain whether the Contractor is complying with the applicable civil rights laws.
  - d) Should a discrimination complaint be filed by a HCFA staff member or contractor alleging an incident claimed to be caused by either the Contractor's staff or one of its subcontractors who are considered to be performing duties under this contract, the Contractor shall work with HCFA to investigate and resolve the allegation. HCFA reserves the right to determine the complaint resolution and corrective action.
  - e) Electronic and Information Technology Accessibility Requirements. The Contractor agrees to comply with the electronic and information technology accessibility requirements under the federal civil rights laws including Section 504 and Section 508 of the Rehabilitation Act of 1973 ("Section 508") and the Americans with Disabilities Act. To comply with these accessibility requirements for Web content and non-Web electronic documents and software, the Contractor shall use W3C's Web Content Accessibility Guidelines ("WCAG") 2.0 AA (For the W3C's guidelines see: <http://www.w3.org/TR/WCAG20/>) (Two core linked resources are Understanding WCAG 2.0 <http://www.w3.org/TR/UNDERSTANDING-WCAG20/> and Techniques for WCAG 2.0 <http://www.w3.org/TR/WCAG20-TECHS/>).
- 1) Should the Contractor have a designated staff member responsible for Contractor's electronic and information technology accessibility compliance, the name and contact information for this individual shall be provided to HCFA within ten (10) days of the implementation of this Contract and within ten (10) days of this position being reassigned to another staff member.
  - 2) Prior to the start of this Contract and on an annual basis thereafter, the Contractor's staff that is designated to work on HCFA's electronic and information technology projects shall receive training on electronic and information technology accessibility requirements. The Contractor shall be able to show documented proof that this training was provided. In addition, Contractor shall provide a copy of its electronic and information technology accessibility training to HCFA upon request.
  - 3) Contractor agrees to perform regularly scheduled (i.e., automatic) scans and manual testing for WCAG 2.0 AA compliance for all user content and applications in order to meet the standards for compliance. The Contractor must ensure that any system additions, updates, changes or modifications comply with WCAG 2.0 AA. COTS products may be used to verify aspects of WCAG 2.0 AA compliance.

- 4) Additionally, the Contractor agrees to comply with Title VI of the Civil Rights Act of 1964. In order to achieve Title VI compliance the Contractor should add a system function that allows users to translate the content into a language other than English. This requirement may be satisfied by the provision of a link to Google translate or other machine translate tool.

**B TERM OF CONTRACT:**

- B.1 This Contract shall be effective on DATE (“Effective Date”) and extend for a period of forty-eight (48) months after the Effective Date (“Term”). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.
- B.2 Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to three (3) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State’s sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of eighty-four (84) months.

**C PAYMENT TERMS AND CONDITIONS:**

- C.1 Maximum Liability In no event shall the maximum liability of the State under this Contract exceed **Written Dollar Amount (\$Number)** (“Maximum Liability”). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.
- C.2 Compensation Firm The payment methodology in Section C.3. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.
- C.3 Payment Methodology The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.
- a) The Contractor’s compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.
  - b) The Contractor shall be compensated based upon the following payment methodology:

Goods or Services Description	Amount (per compensable increment)
Release 1: Project Baseline Review (PBR) – CMS	\$ Number
Release 1: Preliminary Design Consult (PDC) – State	\$ Number
Release 1: Detailed Design Consult (DDC) – State	\$ Number
Release 1: Final Detailed Design Review – CMS	\$ Number
Release 1: Validation Readiness Review (VRR) – State	\$ Number
Release 1: Implementation Readiness Review (IRR) – State	\$ Number
Release 1: Operational Readiness Review (ORR) – CMS	\$ Number
Release 1: Post Implementation Review – State	\$ Number
<b>REPEAT ABOVE GATES FOR ALL PROPOSED RELEASES</b>	\$ Number
Monthly O&M Services—Post Release 1, Month 1	\$ Number
<b>REPEAT ABOVE O&amp;M PAYMENT FOR ALL PROPOSED MONTHS</b>	\$ Number

Goods or Services Description	Amount (per compensable increment)
<b>OF O&amp;M DURING INITIAL CONTRACT PERIOD</b>	
Monthly O&M Services— Year 1	\$ Number
Monthly O&M Services— Year 2	\$ Number
Monthly O&M Services— Year 3	\$ Number

- c) The Contractor shall be compensated for Special Project Change Orders and Enhancement Change Orders requested and performed pursuant to Contract Section A.28 without a formal amendment of this Contract based upon the hourly payment rates detailed in the Cost Proposal, attached to this document as Contract Attachment #8, PROVIDED THAT:
- 1) compensation to the Contractor for Special Project Change Orders shall not exceed FIFTEEN PERCENT (15 %) of the sum of milestone payments detailed in Section C.3.b, above (which is the total cost for the milestones and associated deliverables set forth in the Table of Deliverables).
  - 2) compensation to the Contractor for Enhancement Change Orders shall not exceed the cost associated with TEN PERCENT (10%) of the effort (by Staff Position) for each Release, as detailed in the Cost Proposal.
  - 3) If, at any point during the Term, the State determines that the cost of necessary Special Projects work would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	Amount (per compensable increment)
Special Project Change Order Requests (Section A.28)	\$ _____ (15% of the sum of milestone payments reimbursed at hourly rates submitted in Cost Proposal for multiple staff levels)
Enhancement Change Order Request (Section A.10.13.5)	\$ _____ (Amount contained in the Enhancements Tab of the Cost Proposal reimbursed at hourly rates submitted in Cost Proposal for multiple staff levels)
<b>NOTE: The Contractor shall not be compensated for travel time to the primary location of service provision.</b>	

- C.4 Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

- C.5 Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3, above. If an invoice is for services rendered by Contractor's staff and subcontractors, the invoice shall, at a minimum, include the name of each individual, the individual's job family, the number of hours worked during the period, the applicable Payment Rate, the total compensation requested for the individual, and the total amount due the Contractor for the period invoices. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

Division of Health Care Finance and Administration  
 310 Great Circle Road  
 Nashville, TN 37243

- a) Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):
  - 1) Invoice number (assigned by the Contractor);
  - 2) Invoice date;
  - 3) Contract number (assigned by the State);
  - 4) Customer account name: State Agency & Division Name;
  - 5) Customer account number (assigned by the Contractor to the above-referenced Customer);
  - 6) Contractor name;
  - 7) Contractor Tennessee Edison registration ID number;
  - 8) Contractor contact for invoice questions (name, phone, or email);
  - 9) Contractor remittance address;
  - 10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
  - 11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
  - 12) Applicable payment methodology (as stipulated in Section C.3) of each good or service invoiced;
  - 13) Amount due for each compensable unit of good or service; and
  - 14) Total amount due for the invoice period.
- b) Contractor's invoices shall:
  - 1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;

- 2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
  - 3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
  - 4) Include shipping or delivery charges only as authorized in this Contract.
- c) The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.
- C.6 Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.
- C.7 Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.
- C.8 Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.
- C.9 Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.
- a) The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by Automated Clearing House; and
  - b) The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

## **D MANDATORY TERMS AND CONDITIONS:**

- D.1 Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

- D.2 Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Darin J. Gordon, Deputy Commissioner  
 Department of Finance and Administration  
 Division of Health Care Finance and Administration  
 310 Great Circle Road  
 Nashville, TN 37243  
[Darin.J.Gordin@tn.gov](mailto:Darin.J.Gordin@tn.gov)  
 Telephone # (615) 507-6443  
 FAX # (615) 253-6507

The Contractor:

Contractor Contact Name & Title  
 Contractor Name  
 Address  
 Email Address  
 Telephone # Number  
 FAX # Number

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

All information or data that is necessary for one or more deliverables set forth in this Contract shall be transmitted between HCFA and Contractor via the data transfer method specified in advance by HCFA. This may include, but shall not be limited to, transfer through HCFA's SFTP system. Failure by the Contractor to transmit information or data that is necessary for a deliverable in the manner specified by HCFA, may, at the option of HCFA, result in Liquidated Damages as set forth in Contract Attachment 2.

- D.3 Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.
- D.4 Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

- D.5 Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.
- D.6 Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.
- D.7 Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.
- D.8 Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

- D.9 Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination. In addition, the Contractor shall comply with the provisions of Contract Section E.27 (Nondiscrimination Compliance Requirements) and this Section D.9 shall not be deemed to limit or abridge any requirement set forth in Section E.27.
- D.10 Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.
- a) The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal

immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Contract Attachment 1, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

- b) Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
- c) The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.
- d) The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.
- e) For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

- D.11 Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.
- D.12 Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.13 Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.
- D.14 Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

- D.15 Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.
- D.16 Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act (PPACA) with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.
- D.17 Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.
- D.18 Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.
- D.19 Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract.
- In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.
- D.20 HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

- a) Contractor warrants to the State that it is familiar with the requirements of the

Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

- b) Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.
- c) The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT “protected health information” as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
- d) The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

D.21 Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System (“TCRS”), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member’s retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of “employee/employer” and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22 Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.23 Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

- a) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
- b) have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
- c) are not presently indicted or otherwise criminally or civilly charged by a government

entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

- d) have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

- D.24 Force Majeure. “Force Majeure Event” means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor’s representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor’s performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.
- D.25 State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract. In addition, the Contractor shall comply with the provisions of Contract Section E.16, (Applicable Laws, Rules, Policies and Court Orders), and this Section D.25 shall not be deemed to limit or abridge any requirement set forth in Section E.16.
- D.26 Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 – 407.
- D.27 Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties’ agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

- D.28 Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.
- D.29 Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.30 Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:
- a) any amendment to this Contract, with the latter in time controlling over any earlier amendments;
  - b) this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes Contract Attachments 1 through 7 below;
  - c) any clarifications of or addenda to the Contractor's proposal seeking this Contract;
  - d) the State solicitation, as may be amended, requesting responses in competition for this Contract;
  - e) any technical specifications provided to proposers during the procurement process to award this Contract; and
  - f) the Contractor's response seeking this Contract.

## **E SPECIAL TERMS AND CONDITIONS:**

- E.1 Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.
- E.2 Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. The Contractor shall only use Confidential Information for activities pursuant to and related to the performance of the Contract. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.
- The obligations set forth in this Section shall survive the termination of this Contract.
- E.3 State Ownership of Goods. The State shall have ownership, right, title, and interest in all goods provided by Contractor under this Contract including full rights to use the goods and transfer title in the goods to any third parties.
- E.4 Ownership of Software and Work Products.

a) Definitions.

- 1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial off-the-shelf software which is not developed using State's money or resources.
- 2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State.
- 3) "Rights Transfer Application Software," shall mean any pre-existing application software owned by Contractor or a third party, provided to State and to which Contractor will grant and assign, or will facilitate the granting and assignment of, all rights, including the source code, to State.
- 4) "Third-Party Software," shall mean software not owned by the State or the Contractor.
- 5) "Work Product," shall mean all deliverables exclusive of hardware, such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State during the course of the project using State's money or resources, including Custom-Developed Application Software. If the deliverables under this Contract include Rights Transfer Application Software, the definition of Work Product shall also include such software. Work Product shall not include Contractor-Owned Software or Third-Party Software.

b) Rights and Title to the Software

- 1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license granted under this Contract.
  - 2) All right, title and interest in and to the Work Product, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other intellectual property and other proprietary rights embodied by and arising out of the Work Product, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Work Product, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Work Product. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties.
  - 3) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted under this Contract.
- c) The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others, materials which are similar to or competitive with those that are produced under this Contract.

- E.5 State Furnished Property. The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less reasonable wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.
- E.6 Work Papers Subject to Review. The Contractor shall make all audit, accounting, or financial analysis work papers, notes, and other documentation available for review by the Comptroller of the Treasury or his representatives, upon request, during normal working hours either while the analysis is in progress or subsequent to the completion of this Contract.
- E.7 Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.
- E.8 Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:
- a) No federally appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
  - b) If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
  - c) The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.
- This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by 31 USC § 1352.
- E.9 Intellectual Property. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

E.10 Liquidated Damages.

In the event of a Contract performance failure, the State may, but is not obligated to address such Contract performance failure and/or assess damages (“Liquidated Damages”) in accordance with Attachment 2 of the Contract. The State shall notify the Contractor of any amounts to be assessed as Liquidated Damages. The Parties agree that due to the complicated nature of the Contractor’s obligations under this Contract it would be difficult to specifically designate a monetary amount for a Contract performance failure, as these amounts are likely to be uncertain and not easily proven. Contractor has carefully reviewed the Liquidated Damages contained in Contract Attachment 2 and agrees that these amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of a Liquidated Damages Event, are a reasonable estimate of the damages that would occur from a Contract performance failure, and are not punitive. The Parties agree that although the Liquidated Damages represent the reasonable estimate of the damages and injuries sustained by the State due to the Contract performance failure, they do not include any injury or damage sustained by a third party. The Contractor agrees that the Liquidated Damages are in addition to any amounts Contractor may owe the State pursuant to the indemnity provision or any other sections of this Contract.

The State is not obligated to assess Liquidated Damages as a result of a Contract performance failure before availing itself of any other remedy. In the event of multiple Contract performance failures, the Parties recognize that the cumulative effect of these Contract performance failures may exceed the compensation of Liquidated Damages. In that event, the State may choose to avail itself of any other remedy available under this Contract or at law or equity. The Parties further recognize that the State may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

Without regard to whether the State has imposed Liquidated Damages or pursued any other remedy due to any action or inaction by the Contractor, the State may impose a corrective action plan or similar measure through a Control Memorandum. Such measure is neither punitive nor related to any damages the State might suffer.

E.11 Partial Takeover of Contract. The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a “Partial Takeover”). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State’s exercise of a Partial Takeover shall not alter the Contractor’s other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State’s exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State’s exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.

E.12 Unencumbered Personnel. The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Contract from performing the same or similar services for the State after the termination of this Contract, either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

- E.13 Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law.

- E.14 Federal Funding Accountability and Transparency Act (FFATA). This Contract requires the Contractor to provide supplies or services that are funded in whole or in part by federal funds that are subject to FFATA. The Contractor is responsible for ensuring that all applicable requirements, including but not limited to those set forth herein, of FFATA are met and that the Contractor provides information to the State as required.

The Contractor shall comply with the following:

- a) Reporting of Total Compensation of the Contractor's Executives.
  - 1) The Contractor shall report the names and total compensation of each of its five most highly compensated executives for the Contractor's preceding completed fiscal year, if in the Contractor's preceding fiscal year it received:

- 2) 80 percent or more of the Contractor's annual gross revenues from federal procurement contracts and federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and
- 3) \$25,000,000 or more in annual gross revenues from federal procurement contracts (and subcontracts), and federal financial assistance subject to the Transparency Act (and subawards); and
- 4) The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 USC 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986. (To determine if the public has access to the compensation information, see the U.S. Security and Exchange Commission total compensation filings at <http://www.sec.gov/answers/execomp.htm>).

As defined in 2 C.F.R. § 170.315, "Executive" means officers, managing partners, or any other employees in management positions.

- b) Total compensation means the cash and noncash dollar value earned by the executive during the Contractor's preceding fiscal year and includes the following (for more information see 17 C.F.R. § 229.4021(2)):
  - 1) Salary and bonus.
  - 2) Awards of stock, stock options, and stock appreciation rights. Use the dollar amount recognized for financial statement reporting purposes with respect to the fiscal year in accordance with the Statement of Financial Accounting Standards No. 123 (Revised 2004) (Financial Accounting Standards 123R), Shared Based Payments.
  - 3) Earnings for services under non-equity incentive plans. This does not include group life, health, hospitalization or medical reimbursement plans that do not discriminate in favor of executives, and are available generally to all salaried employees.
  - 4) Change in pension value. This is the change in present value of defined benefit and actuarial pension plans.
  - 5) Above-market earnings on deferred compensation which is not tax qualified.
  - 6) Other compensation, if the aggregate value of all such other compensation (e.g. severance, termination payments, value of life insurance paid on behalf of the employee, perquisites or property) for the executive exceeds \$10,000.
- c) The Contractor must report executive total compensation described above to the State by the end of the month during which this Contract is awarded.
- d) If this Contract is amended to extend the Term, the Contractor must submit an executive total compensation report to the State by the end of the month in which the term extension becomes effective.
- e) The Contractor will obtain a Data Universal Numbering System (DUNS) number and maintain its DUNS number for the term of this Contract. More information about obtaining a DUNS Number can be found at: <http://fedgov.dnb.com/webform/>

The Contractor's failure to comply with the above requirements is a material breach of this Contract for which the State may terminate this Contract for cause. The State will not

be obligated to pay any outstanding invoice received from the Contractor unless and until the Contractor is in full compliance with the above requirements.

- E.15 Survival. The terms, provisions, representations, and warranties contained in Sections D.11 (Records), D.19 (Hold Harmless), D.20 (HIPAA Compliance), E.2 (Confidentiality of Records), E.7 (Prohibited Advertising), E.9 (Intellectual Property) E.13 (Personally Identifiable Information), E.19 (Notification of Breach), E.21 (SSA Data), and E.25 (IRS Data) of this Contract shall survive the completion of performance, termination or expiration of this Contract.
- E.16 Applicable Laws, Rules, Policies and Court Orders. The Contractor agrees to comply with all applicable federal and State laws, rules, regulations, sub-regulatory guidance including but not limited to the State Medicaid Manual, executive orders, HCFA waivers, and all current, modified or future Court decrees, orders or judgments applicable to the State's TennCare and CHIP programs. Such compliance shall be performed at no additional cost to the State.
- E.17 Business Associate. Contractor hereby acknowledges its designation as a business associate under HIPAA and agrees to comply with all applicable HIPAA regulations. In accordance with the HIPAA regulations, the Contractor shall, at a minimum:
- a) Comply with requirements of the HIPAA, including, but not limited to, the transactions and code sets, privacy, security, and identifier regulations. Compliance includes meeting all required transaction formats and code sets with the specified data sharing agreements required under the regulations;
  - b) Transmit/receive from/to its providers, subcontractors, clearinghouses and HCFA all transactions and code sets required by HIPAA in the appropriate standard formats, utilizing appropriate and adequate safeguards, as specified under the law and as directed by HCFA so long as HCFA direction does not conflict with the law;
  - c) Agree that if it is not in compliance with all applicable standards defined within the transactions and code sets, privacy, security and all subsequent HIPAA standards, that it will be in breach of this Contract and will then take all reasonable steps to cure the breach or end the violation as applicable. Since inability to meet the transactions and code sets requirements, as well as the privacy and security requirements can bring basic business practices between HCFA and the Contractor and between the Contractor and its providers and/or subcontractors to a halt, if for any reason the Contractor cannot meet the requirements of this Section, HCFA may terminate this Contract.
  - d) Ensure that Protected Health Information (PHI) exchanged between the Contractor and HCFA is used only for the purposes of treatment, payment, or health care operations and health oversight and its related functions. All PHI not transmitted for these purposes or for purposes allowed under the federal HIPAA regulations shall be de-identified to secure and protect the individual enrollee's PHI;
  - e) Report to HCFA's Privacy Office immediately upon becoming aware of any use or disclosure of PHI in violation of this Contract by the Contractor, its officers, directors, employees, subcontractors or agents or by a third party to which the Contractor disclosed PHI;
  - f) Specify in its agreements with any agent or subcontractor that will have access to PHI that such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to the Contractor pursuant to this Section;
  - g) Make its internal policies and procedures, records and other documentation related

to the use and disclosure of PHI available upon request to the U.S. Secretary of Health and Human Services for the purposes of determining compliance with the HIPAA regulations;

- h) Create and adopt policies and procedures to periodically audit adherence to all HIPAA regulations;
- i) Agree to ensure that any agent, including a subcontractor, to whom it provides PHI that was created, received, maintained, or transmitted by or on behalf of HCFA agrees to use reasonable and appropriate safeguards to protect the PHI.
- j) If feasible, return or destroy all PHI, in whatever form or medium (including any electronic medium) and all copies of any data or compilations derived from and allowing identification of any individual who is a subject of that PHI upon termination, cancellation, expiration or other conclusion of the Agreement, and in accordance with this Section of this Contract. The Contractor shall complete such return or destruction as promptly as possible, but not later than thirty (30) days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement. The Contractor shall identify any PHI that cannot feasibly be returned or destroyed. Within such thirty (30) days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement, the Contractor shall: (1) certify an oath in writing that such return or destruction has been completed; (2) identify any PHI which cannot feasibly be returned or destroyed; and (3) certify that it will only use or disclose such PHI for those purposes that make its return or destruction infeasible;
- k) Implement all appropriate administrative, physical and technical safeguards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this Contract and, including, but not limited to, privacy, security and confidentiality requirements in 45 CFR Parts 160 and 164;
- l) Set up appropriate mechanisms to limit use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure;
- m) Create and implement policies and procedures to address present and future HIPAA regulatory requirements as needed, including, but not limited to: use and disclosure of data; de-identification of data; minimum necessary access; accounting of disclosures; enrollee's right to amend, access, request restrictions; notice of privacy practices and right to file a complaint;
- n) Provide an appropriate level of training to its staff and employees regarding HIPAA related policies, procedures, enrollee rights and penalties prior to the HIPAA implementation deadlines and at appropriate intervals thereafter;
- o) Track training of Contractor staff and employees and maintain signed acknowledgements by staff and employees of the Contractor's HIPAA policies;
- p) Be allowed to use and receive information from HCFA where necessary for the management and administration of this Contract and to carry out business operations where permitted under the regulations;
- q) Be permitted to use and disclose PHI for the Contractor's own legal responsibilities;
- r) Adopt the appropriate procedures and access safeguards to restrict and regulate access to and use by Contractor employees and other persons performing work for

the Contractor to have only minimum necessary access to PHI and personally identifiable data within their organization;

- s) Continue to protect and secure PHI and personally identifiable information relating to enrollees who are deceased; and
- t) Track all security incidents as defined by HIPAA and periodically report such incidents to HCFA in summary fashion.

- E.18 Information Holders. HCFA and the Contractor are “information holders” as defined in TCA 47-18-2107. In the event of a breach of the security of Contractor’s information system, as defined by TCA 47-18-2107, the Contractor shall indemnify and hold HCFA harmless for expenses and/or damages related to the breach. Such obligations shall include, but not be limited to, mailing notifications to affected enrollees. Substitute notice to written notice, as defined by TCA 47-18-2107(e)(2) and (3), shall only be permitted with HCFA’s express written approval. The Contractor shall notify HCFA’s Privacy Office immediately upon becoming aware of any security incident that would constitute a “breach of the security of the system” as defined in TCA 47-18-2107.
- E.19 Notification of Breach and Notification of Suspected Breach. - The Contractor shall notify HCFA’s Privacy Office immediately upon becoming aware of any incident, either confirmed or suspected, that represents or may represent unauthorized access, use or disclosure of encrypted or unencrypted computerized data that materially compromises the security, confidentiality, or integrity of enrollee PHI maintained or held by the Contractor, including any unauthorized acquisition of enrollee PHI by an employee or otherwise authorized user of the Contractor’s system. This includes, but is not limited to, loss or suspected loss of remote computing or telework devices such as laptops, PDAs, Blackberrys or other Smartphones, USB drives, thumb drives, flash drives, CD-Rs, and/or disks.
- E.20 Transmission of Contract Deliverables. All information or data that is necessary for one or more deliverable set forth in this Contract shall be transmitted between HCFA and Contractor via the data transfer method specified in advance by HCFA. This may include, but shall not be limited to, transfer through HCFA’s SFTP system. Failure by the Contractor to transmit information or data that is necessary for a deliverable in the manner specified by HCFA, may, at the option of HCFA, result in liquidated damages as set forth in Contract Attachment 2.
- E.21 Social Security Administration (SSA) Required Provisions for Data Security. The Contractor shall comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 USC 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 USC §3541, *et seq.*), and related National Institute of Standards and Technology guidelines. In addition, the Contractor shall have in place administrative, physical, and technical safeguards for data.
- a) The Contractor shall not duplicate in a separate file or disseminate, without prior written permission from HCFA, the data governed by the Contract for any purpose other than that set forth in this Contract for the administration of the HCFA program. Should the Contractor propose a redisclosure of said data, the Contractor must specify in writing to HCFA the data the Contractor proposes to redisclose, to whom, and the reasons that justify the redisclosure. HCFA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the administration of the HCFA program.
  - b) The Contractor agrees to abide by all relevant federal laws, restrictions on access, use, and disclosure, and security requirements in this Contract.

- c) The Contractor shall provide a current list of the employees of such contractor with access to SSA data and provide such lists to HCFA.
- d) The Contractor shall restrict access to the data obtained from HCFA to only those authorized employees who need such data to perform their official duties in connection with purposes identified in this Contract. The Contractor shall not further duplicate, disseminate, or disclose such data without obtaining HCFA's prior written approval.
- e) The Contractor shall ensure that its employees:
  - 1) properly safeguard PHI/PII furnished by HCFA under this Contract from loss, theft or inadvertent disclosure;
  - 2) understand that they are responsible for safeguarding this information at all times, regardless of whether or not the Contractor employee is at his or her regular duty station;
  - 3) ensure that laptops and other electronic devices/media containing PHI/PII are encrypted and/or password protected;
  - 4) send emails containing PHI/PII only if encrypted or if to and from addresses that are secure; and,
  - 5) limit disclosure of the information and details relating to a PHI/PII loss only to those with a need to know.

Contractor employees who access, use, or disclose HCFA or HCFA SSA-supplied data in a manner or purpose not authorized by this Contract may be subject to civil and criminal sanctions pursuant to applicable federal statutes.

- f) Loss or Suspected Loss of Data—If an employee of the Contractor becomes aware of suspected or actual loss of PHI/PII, he or she must immediately contact HCFA immediately upon becoming aware to report the actual or suspected loss. The Contractor will use the Loss Worksheet located at [http://www.tn.gov/assets/entities/tenncare/attachments/phi\\_piiworksheet.pdf](http://www.tn.gov/assets/entities/tenncare/attachments/phi_piiworksheet.pdf) to quickly gather and organize information about the incident. The Contractor must provide HCFA with timely updates as any additional information about the loss of PHI/PII becomes available.

If the Contractor experiences a loss or breach of said data, HCFA will determine whether or not notice to individuals whose data has been lost or breached shall be provided and the Contractor shall bear any costs associated with the notice or any mitigation.

- g) HCFA may immediately and unilaterally suspend the data flow under this Contract, or terminate this Contract, if HCFA, in its sole discretion, determines that the Contractor has: (1) made an unauthorized use or disclosure of HCFA SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this Contract.
- h) This Section further carries out Section 1106(a) of the Act (42 USC 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy of 1974 (5 USC 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget ("OMB") guidelines, the Federal Information Security Management Act of 2002 (44 USC 3541 et seq.), and related National Institute of Standards and Technology ("NIST") guidelines, which

provide the requirements that the SSA stipulates that the Contractor must follow with regard to use, treatment, and safeguarding data in the event data is exchanged with a federal information system.

6) Definitions

- i) "SSA-supplied data" – information, such as an individual's social security number, supplied by the Social Security Administration to HCFA to determine entitlement or eligibility for federally-funded programs (CMPPA between SSA and F&A; IEA between SSA and HCFA).
- ii) "Protected Health Information/Personally Identifiable Information" (PHI/PII)(45 C.F.R. 160.103; OMB Circular M-06-19) – Protected health information means individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
- iii) "Individually Identifiable Health Information"– information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- iv) "Personally Identifiable Information" – any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, date and place of birth, mother's maiden name, biometric records, including any other personal information which can be linked to an individual.

E.22 Medicaid and CHIP - The Contractor must provide safeguards that restrict the use or disclosure of information concerning applicants and beneficiaries to purposes directly connected with the administration of the plan:

- a) Purposes directly related to the administration of Medicaid and CHIP include:
  - 1) establishing eligibility;
  - 2) determining the amount of medical assistance;
  - 3) providing services for beneficiaries; and,
  - 4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to Medicaid or CHIP administration.
- b) The Contractor must have adequate safeguards to assure that:
  - 1) Information is made available only to the extent necessary to assist in the valid administrative purposes of those receiving the information, and information

- 2) received under 26 USC is exchanged only with parties authorized to receive that information under that section of the Code; and, the information is adequately stored and processed so that it is protected against unauthorized disclosure for other purposes.
- c) The Contractor must have criteria that govern the types of information about applicants and beneficiaries that are safeguarded. This information must include at least--
- 1) Names and addresses;
  - 2) Medical services provided;
  - 3) Social and economic conditions or circumstances;
  - 4) Contractor evaluation of personal information;
  - 5) Medical data, including diagnosis and past history of disease or disability
  - 6) Any information received for verifying income eligibility and amount of medical assistance payments, including income information received from SSA or the Internal Revenue Service;
  - 7) Income information received from SSA or the Internal Revenue Service must be safeguarded according to Medicaid and CHIP requirements;
  - 8) Any information received in connection with the identification of legally liable third party resources; and.
  - 9) Social Security Numbers.
- d) The Contractor must have criteria approved by HCFA specifying:
- 1) the conditions for release and use of information about applicants and beneficiaries:
  - 2) Access to information concerning applicants or beneficiaries must be restricted to persons or Contractor representatives who are subject to standards of confidentiality that are comparable to those of HCFA;
  - 3) The Contractor shall not publish names of applicants or beneficiaries;
  - 4) The Contractor shall obtain permission from a family or individual, whenever possible, before responding to a request for information from an outside source, unless the information is to be used to verify income, eligibility and the amount of medical assistance payment to an authorized individual or entity;
  - 5) If, because of an emergency situation, time does not permit obtaining consent before release, the Contractor shall notify HCFA, the family or individual immediately after supplying the information.
  - 6) The Contractor's policies must apply to all requests for information from outside sources, including governmental bodies, the courts, or law enforcement officials.
    - i) The Contractor shall notify HCFA of any requests for information on applicants or beneficiaries by other governmental bodies, the courts or law enforcement officials ten (10) days prior to releasing the requested information.

- 7) If a court issues a subpoena for a case record or for any Contractor representative to testify concerning an applicant or beneficiary, the Contractor must notify HCFA at least ten (10) days prior to the required production date so HCFA may inform the court of the applicable statutory provisions, policies, and regulations restricting disclosure of information.
- 8) The Contractor shall not request or release information to other parties to verify income, eligibility and the amount of assistance under Medicaid or CHIP, prior to express approval from HCFA.
- E.23 Employees Excluded from Medicare, Medicaid or CHIP. The Contractor does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly employ, in the performance of this Contract, employees who have been excluded from participation in the Medicare, Medicaid, and/or CHIP programs pursuant to Sections 1128 of the Social Security
- E.24 Offer of Gratuities. By signing this contract, the Contractor signifies that no member of or a delegate of Congress, nor any elected or appointed official or employee of the State of Tennessee, the federal General Accounting Office, federal Department of Health and Human Services, the CMS, or any other state or federal agency has or will benefit financially or materially from this Contract. This Contract may be terminated by HCFA as provided in Section D.6, if it is determined that gratuities of any kind were offered to or received by any of the aforementioned officials or employees from the Contractor, its agent, or employees.
- E.25 Internal Revenue Service (IRS) Safeguarding Of Return Information:
- a) Performance - In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
    - 1) This provision shall not apply if information received or delivered by the Parties under this Contract is NOT "federal tax returns or return information" as defined by IRS Publication 1075 and IRC 6103.
    - 2) All work will be done under the supervision of the contractor or the contractor's employees. The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
    - 3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
    - 4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
    - 5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

- 6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- 7) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- 8) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
- 9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- 10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
  - b) Criminal/Civil Sanctions
    - 1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
    - 2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

- 3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 USC 552a. Specifically, 5 USC 552a(i)(1), which is made applicable to contractors by 5 USC 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- 4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Publication 1075 Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Publication 1075 Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Publication 1075 Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

Inspection - The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safe.

- E.26 Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to RFQ 32101-15557 (RFQ Attachment B, Section B.15) and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.

**IN WITNESS WHEREOF,**

**CONTRACTOR LEGAL ENTITY NAME:**

---

**CONTRACTOR SIGNATURE**

**DATE**

---

**PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)**

**DEPARTMENT OF FINANCE AND ADMINISTRATION  
DIVISION OF HEALTH CARE FINANCE AND ADMINISTRATION:**

---

**NAME & TITLE**

**DATE**

## Contract ATTACHMENT 1

**ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE**

<b>SUBJECT CONTRACT NUMBER:</b>	
<b>CONTRACTOR LEGAL ENTITY NAME:</b>	
<b>FEDERAL EMPLOYER IDENTIFICATION NUMBER: (or Social Security Number)</b>	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

**CONTRACTOR SIGNATURE**

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

**PRINTED NAME AND TITLE OF SIGNATORY****DATE OF ATTESTATION**

**Contract ATTACHMENT 2****LIQUIDATED DAMAGES**

In the event of a Contract performance failure by Contractor and such Contract performance failure is not included in the following table with an associated Liquidated Damage amount, the parties hereby agree that the State may choose one of the following courses of action in order to obtain redressability for such Contract performance failure: (1) the State may assess actual damages resulting from the Contract performance failure against the Contractor in the event that such actual damages are known or are reasonably ascertainable at the time of discovery of such Contract performance failure or (2) if such actual damages are unknown or are not reasonably ascertainable at the time of discovery of the Contract performance failure, the State may (a) require the Contractor to submit a corrective action plan to address any such Contract performance failure and/or (b) assess a liquidated damage against Contractor for an amount that is reasonable in relation to the Contract performance failure as measured at the time of discovery of the Contract performance failure. In the event that the State chooses to assess a Liquidated Damage for a Contract performance failure according to the immediately preceding sentence, in no event shall such Liquidated Damage be in excess of \$1,000 for any single Contract performance failure. HCFA may elect to apply the following liquidated damages remedies in the event the Contractor fails to perform its obligations under this Contract in a proper and/or timely manner. Upon determination by HCFA that the Contractor has failed to meet any of the requirements of this Contract in a proper and/or timely manner, HCFA will notify the Contractor in writing of the deficiency and of the potential liquidated damages to be assessed. Should the deficiency remain uncorrected for more than thirty (30) calendar days from the date of the original notification of the deficiency by HCFA, HCFA may impose an additional liquidated damage of Five Hundred Dollars (\$500) per day from the date of the original notification to Contractor until said deficiency is resolved.

All liquidated damages remedies set forth in the following table may, at HCFA's election, be retroactive to the date of the initial occurrence of the failure to comply with the terms of the Contract as set forth in the notice of deficiency from HCFA and may continue until such time as the HCFA Deputy Commissioner determines the deficiency has been cured.

If liquidated damages are assessed, HCFA shall reduce the amount of any payment due to the Contractor in the next invoice by the amount of damages. In the event that damages due exceed the amount HCFA is to pay to Contractor in a given payment, HCFA shall invoice Contractor for the amount exceeding the amount payable to Contractor, and such excess amount shall be paid by Contractor within thirty (30) calendar days of the invoice date. In situations where the Contractor wishes to dispute any liquidated damages assessed by HCFA, the Contractor must submit a written notice of dispute, including the reasons for disputing the liquidated damages, within thirty (30) calendar days of receipt of the notice from HCFA containing the total amount of damages assessed against the Contractor. If the Contractor fails to timely dispute a liquidated damages assessment as set forth herein, such failure shall constitute a bar to the Contractor seeking to have the assessment amount overturned in a forum or court of competent jurisdiction.

Liquidated damages will apply in the below defect occurrences. Contractor acknowledges that the actual damages likely to result from breach of the below SLRs are difficult to estimate and may be difficult for the State to prove. The parties intend that the Contractor's payment of assessed liquidated damages will compensate the State for material breach by the Contractor obligations under this Contract. Liquidated damages do not serve as punishment for any breach by the Contractor.

Defect severity will be assigned according to the following criteria:

*Table 6: Defect Severity*

<b>Severity</b>	<b>Description</b>
<b>Critical</b>	A complete failure of the Solution application or supported process in the Production Instance has occurred. There is no work around for the problem. A majority of end users of the Production Instance are affected or an entire business division is affected or the outage has occurred during a critical business process or period, such as end of month or end of year processing. Critical defects take precedence over all other requests.
<b>High</b>	Major issues exist within the Solution or supported process in the Production Instance. The issue affects large portions of the user community. This includes high visibility issues involving upper management or time sensitive issues. An example of this priority level is an impact to multiple users of the system, or an inability to process applicants.
<b>Medium</b>	Issues exist with an application or supported process in the Production Instance that affects a few users on a regular basis, thereby preventing some work from being accomplished. Examples of this type of priority would be inability to access implemented functionality or implemented functionality not operating as it should.
<b>Low</b>	An informational inquiry or nonrecurring issue exists with the Production Instance that affects a few non-critical users or processes. Workarounds are readily available.

Table 7: Tennessee Eligibility Determination System - Service Level Requirements (SLR)

SLR #	Service Level Requirement Category	Service Level Requirement Name	Required Service Level	Description	Liquidated Damage
1.1	Production Services	Account Transfers	Within one calendar day of scheduled process time	Successfully execute daily account transfer process between FDSH and TEDS.	Five hundred dollars (\$500) per calendar day per account for each account not successfully transferred between the TEDS and FDSH within twenty four (24) hours of its scheduled process time (excludes transfers that fail due to FDSH system failure). The maximum cap on this LD shall be fifty thousand dollars (\$50,000) per day.
1.2	Production Services and Output Management	Notice/Letter Generation	< forty-eight (48) Hours of event triggering letter/notice. If forty-eight (48) hours falls during a period when the USPS is not accepting deliveries, the letter/notice must be delivered to the USPS within eight (8) hours of the USPS opening.	Letters/notices are produced, printed, folded/inserted, and delivered to the USPS. This SLR excludes large (distributions over one million (1,000,000)) letter/notice distributions covered in Section A.17.17.1.10.c of the Contract, which shall follow the defined schedule.	One hundred dollars (\$100) per notice/letter per USPS service day until the correspondence is produced, printed, folded/inserted and delivered to the USPS. The maximum cap on this LD shall be fifty thousand dollars (\$50,000) per day.
2.1	Reporting Requirements	Daily Operations Report	By noon (12:00pm) the following day	Provide a timely and accurate Daily Operations Report	Five hundred dollars (\$500) per clock hour for each clock hour after noon (12:00pm) that an accurate and complete report is not received, unless waived by HCFA. If the report is received on time but the information reported is inaccurate or incomplete, HCFA may assess up to five hundred dollars (\$500) per clock hour until an acceptable report is received, not to exceed ten thousand dollars (\$10,000) per day.
3.1	System Availability and Reliability	System Uptime	> ninety-nine point nine percent (99.9%) available	The availability of the main TEDS customer interface. Number of hours that the Contractor web site is operational and capable of performing all functions. Excluding scheduled system outages. <i>Note: &lt; forty three point two (43.2) minutes of allowable downtime for thirty (30)-day</i>	Two hundred fifty dollars per minute (\$250) for every minute below than the contracted target level of availability for the month.

SLR #	Service Level Requirement Category	Service Level Requirement Name	Required Service Level	Description	Liquidated Damage
				<i>month</i>	
4.1	Technical Operations	Defect Resolution Time	<p>Defect Resolution Time: Low priority – twelve (12) Business hours*</p> <p>Medium priority – eight (8) Business hours*</p> <p>High priority – one (1) Clock hour**</p> <p>Critical priority – thirty (30) Clock minutes***</p>	<p>Defect Resolution Time measures the Contractor's time to resolution of incidents based upon critical, high, medium, and low priorities.</p> <p>* Business hours = 8:00 a.m. – 5:00 p.m., Monday – Friday, except State holidays</p> <p>** Clock hours = clock time</p> <p>*** Clock minutes = clock time</p>	<p>The damages vary by criticality of the incident and are:</p> <p>Fifty dollars (\$50) per low incident per business hour above four (4) Business hours,</p> <p>Fifty dollars (\$50) per medium incident per business hour above two (2) Business hours*,</p> <p>Fifty dollars (\$50) per high incident per clock hour above one (1) Clock hour**,</p> <p>Fifty dollars (\$50) per critical incident per clock minute above thirty (30) Clock minutes***.</p> <p>The LD amount for defect resolution time shall not exceed (for all incidents) thirty thousand dollars (\$30,000) per month.</p>
4.2	Technical Operations	Solution File Backup and Restoration	For 24/7/365 requests, file restoration services are to be ninety-five percent (95%) within four (4) hours, and one hundred percent (100%) within twenty-four (24) hours. Restoration from daily and weekly backups will be capable of initiation within four (4) hour of request, and completed within eight (8) hours of request.	In the event of any failed storage for 24/7/365 service level data, ninety-five percent (95%) of files will be restored from backup within four (4) hours, and one hundred (100%) will be restored within twenty-four (24) hours. Restoration from backups must be capable of initiation within one (1) hour of request and completed within four (4) hours of request.	<p>Two thousand five hundred dollars (\$2,500) per failure to meet either the ninety-five percent (95%) threshold or the one hundred percent (100%) threshold (note that only one (1) LD per occurrence).</p> <p>Two thousand five hundred dollars (\$2,500) per backup initiation not complete within four (4) hours of request.</p>
4.3	Technical Operations	Interfaces	Incoming interface transaction data is correct and sufficient to perform the required transaction.	System is able to request, receive, and process accurate data updated on the required schedule from all incoming interfaces from FDSH, IRS, SSA and State systems. All outgoing interfaces shall provide accurate and complete data, as entered by users, to the partner interfaces, as required for the required transaction.	One thousand dollars (\$1,000) per calendar day per interface that the system is not able to request, receive, and accurately process. The Contractor shall not be responsible for interface technical problems that are caused by interface source.

SLR #	Service Level Requirement Category	Service Level Requirement Name	Required Service Level	Description	Liquidated Damage
5.1	Performance	Application Response Times	Less than two (2) seconds ninety-five percent (95%) of the time.	The Solution shall maintain an application response time of less than two (2) seconds ninety-five percent (95%) of the time, for any user action. No action or page load shall have response times of more than three (3) seconds. The Solution component and system shall be considered as unavailable if the online response time is a factor of three (3) greater than Application Response Time SLR. In this case, Liquidated Damages associated with SLR #3.1 above (System Availability) shall apply.	Five thousand dollars (\$5,000) per percentage point that exceeds the Application Response Time SLR timeframe. Not to exceed thirty thousand dollars (\$30,000) per month.
6.1	Security and Privacy	Privacy Incident Reporting	Immediately, not to exceed one (1) hour after awareness of incident.	Any Solution privacy incident involving sensitive data shall be reported, in accordance with HCFA privacy and security protocols for incident response, to the HCFA Privacy Office immediately and not to exceed one (1) hour after awareness of incident. For these purposes, a Privacy Incident is defined as, but not limited to: a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an unauthorized purpose, have access or potential access to PII/PHI/FTI in usable form, whether physical or electronic.	One thousand (\$1,000) per hour (following the first hour) between Privacy Incident and written report of the breach to the HCFA Privacy Office.

*Table 8: Incident Resolution*

Severity	Time from receipt of State notice to CAP Approval	Liquidated Damages failure to complete an accepted CAP within allotted time	Liquidated Damages for subsequent occurrences of substantially the same issue, first 3 occurrences after CAP approval	Liquidated Damages for subsequent occurrences of substantially the same issue (for over 3 occurrences)
----------	---	---	---	--

<b>Severity</b>	<b>Time from receipt of State notice to CAP Approval</b>	<b>Liquidated Damages failure to complete an accepted CAP within allotted time</b>	<b>Liquidated Damages for subsequent occurrences of substantially the same issue, first 3 occurrences after CAP approval</b>	<b>Liquidated Damages for subsequent occurrences of substantially the same issue (for over 3 occurrences)</b>
<b>Critical</b>	Fewer than 24 clock hours	Five hundred dollars (\$500) for each additional clock hour	Twenty-five thousand dollars (\$25,000) per incident	Seventy-five thousand dollars (\$75,000) per incident
<b>High</b>	Fewer than 48 clock hours	Five hundred dollars (\$500) for each additional clock hour	Twelve thousand five hundred dollars (\$12,500) per incident	Thirty-seven thousand five hundred dollars (\$37,500) per incident
<b>Medium</b>	Fewer than 3 days	Five hundred dollars (\$500) for each additional day	Two thousand five hundred dollars (\$2,500) per incident	Seven thousand five hundred dollars (\$7,500) per incident

## Contract ATTACHMENT 3

## LIST OF NOTICES

The following is a list includes, but is not limited to, the Eligibility Operations Notices that shall be utilized by the State of Tennessee for the TEDS.

*Table 9: Eligibility Operations – TC*

TC Letter ID	Description Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
Q3	Demographic - Address Change Letter	Daily	10000
H5	Demographic -Temporary Reinstatement of Eligibility	Daily	2
H6	Demographic - Adding Members to case	Daily	0
P6	Demographic - Date of Birth change	Daily	167
P8	Demographic - SSN change	Daily	2441
207	Creditable Coverage Certificate - Daily	Daily	268
058a	Involuntary Termination - has access to health insurance or has health insurance	Daily	0
061	Voluntary Termination - recip "asked"	Daily	1367
058c	Involuntary Termination - recip out of state	Daily	151
250a	Medicaid appr, new add or less than 62 day break, with MCO change option	Daily	5000
250b	Medicaid appr new or greater than 62 break with MCO change option	Daily	7900
250c	Medicaid approval as presumptive (pregnant) with MCO change option	Daily	1238
250d	Presumptive appr (pregnant) given 45 days with MCO change option	Daily	179
251a	Redetermination appr with copays; no MCO change option	Weekly	
251b	Redetermination appr without copays; no MCO change option	Weekly	
251c	Medicaid Eligibility Redetermination appr without copays; no MCO change option	Weekly	
251d	ME Redetermination appr with copays; no MCO change option	Weekly	
252a	New ME, rollover from Mcaid, Uninsured, income btwn 100-199% FPL appr, with copays; no MCO change option	Weekly	
252b	New ME, rollover from Mcaid, appr no copays; no MCO change option	Weekly	
252c	New ME, rollover from Mcaid, income is above 200%, appr with copays; no MCO change option	Weekly	
254	SSI Approval - Child is now SSI - new add	Daily	143

Table 10: Eligibility Operations – TEDS

<b>TEDS Letter ID</b>	<b>Description (Policy – Letter Title)</b>	<b>Current or Planned Frequency</b>	<b>Monthly Volume (Where Applicable)</b>
300	TEDS - Emergency - Alien approval for medical care	Daily	
301	TEDS - Denial for TCM, TCS, CoverKids,HealthyTNBabies	Daily	
301a, 301b	Denials produced by TEAMS that may convert to TEDS	Daily	
301c	TEDS - Denied due to No Response	Bi-Monthly	2900
302	TEDS - Authorized rep change	Daily	
303	TEDS - Generic change notice	Daily	
304	TEDS - Citizenship verification - Approved for 90 days , TCM, CoverKids	Daily	
305	TEDS - Electronic notice selection	Daily	
306	TEDS - TCM CHOICES - Patient Liability - increase - decrease	Daily	
307	TEDS - Request for verification	Daily	
307a	Special mailing - EOG -Request for verification of income	Weekly or Bi-Weekly	3500
307b	Special mailing - EOG - Request for verification of citizenship	Weekly or Bi-Weekly	4
307c	Special mailing - EOG - Request for verification of income and citizenship	Weekly or Bi-Weekly	1484
308	TEDS – Qualified Medicare Beneficiary, Specified Low Income Medicare Beneficiaries, Qualified Disabled Working Individual, QI-1 denial	Daily	
309	TEDS - Out of state - 10 day response	Daily	
310	TEDS - Portal Password has changed	Daily	
311	TEDS - Cover page - resending a letter you requested.	Daily	
312	TEDS – Third Party Liability (TPL) verification	Daily	
313	TEDS - Application withdrawl	Daily	
314	TEDS - Confirmation that your application was received and in process	Daily	
315Ti	TEDS - Involuntary Term notices - 058a and 058c and many other terms with different variables	Daily	
316	TEDS - Spend Down requesting information	Daily	
317	TEDS -Spend Down needing additional information	Daily	
318	TEDS - Failed electronic letter delivery	Daily	
350	TEDS - Approval - CoverKids, HealthyTNBabies (CHIP approval)	Daily	
35–b - (replaces TN 250C)	TEDS -Batch presumptive pregnant	Daily	
351d (replaces TN 250C)	TEDS -Desktop at DOH presumptive pregnant	Daily	
352b	TEDS - Batch – Breast and Cervical Cancer (BCC) presumptive	Daily	
352d	TEDS - Desktop - at DOH - BCC presumptive	Daily	

TEDS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
353	TEDS - Approval - Medicare Savings Program	Daily	
354	TEDS - Approval for BCC and Pregnant	Daily	
355	TEDS - Term notice due to reverification - you re- applied and are denied	Daily	

*Table 11: Eligibility Operations – Renewal*

Renewal Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
401	Renewal - MAGI Initial letter with renewal packet	Monthly	
401R	Renewal - Reprint of Initial letter with renewal packet	Daily	
401a	Renewal - Long Term Services and Supports (LTSS) Initial letter with renewal packet	Monthly	
401AR	Renewal - Reprint of LTSS letter with NM renewal packet	Daily	
402	Redetermination - Approved for TennCare Medicaid	Daily	
402a	Redetermination - Approved for TennCare Medicaid - during the 90 day reconsideration period - produced by interChange	Daily	
403	Redetermination - Approval for Medicare Savings Program (MSP)	Daily	
404	Redetermination - Approved for TennCare Standard	Daily	
405	Redetermination - Approved for CoverKids - effective date to be included	Daily	
405a	Redetermination - Approved for CoverKids - renewal received after coverage ended	Daily	
406	Redetermination - Cover page which proceeds all TN 406 letters with barcode that tracks back to the recipient that was mailed the letter	Daily	
406a	Renewal - need more information - Household Income	Daily	
406b	Renewal - need more information - Citizenship or Immigration status and Household Income	Daily	
406c	Renewal - need more information - Citizenship or Immigration status	Daily	
406d	Renewal - need more information - proof that you live in Tennessee	Daily	
406e	Renewal - need more information - SSN or proof that you have applied for SSN	Daily	
406f	Renewal - need more information - household income, including spousal support alimony payments (for Transitional/Extended)	Daily	
406g	Renewal - need more information - do you have or can get insurance through your job or a family members job	Daily	
406h	Renewal - your renewal packet was received, but not signed	Daily	
406i	Renewal - need more information - tell us about health problems, check for Medical Eligibility "ME" to apply for STD	Daily	
406j	Renewal - need more information - do you have insurance for pregnancy care, maternity benefits (CHIP only)	Daily	

Renewal Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
406k	Renewal - need more information - missing ME packet information	Daily	
407	Renewal - packet received but you were not selected for renewal, or not currently enrolled	Daily	
408	Renewal - Denied, 20 day term - you applied and we have determined you no longer qualify for TC, Medicaid Savings Program (MSP), CK	Daily	
408ftp	Renewal - Denied, 20 day term - renewal packet received, we requested more information and you did not give us what we requested for TC, MSP, CK	Daily	
409	Renewal - Denied during 90 day reconsideration period - you do not qualify for TC, MSP or CK	Daily	
409ftp	Renewal - Denied during 90 day reconsideration period - renewal packet received, we requested more information, you did not give us what we requested for TC, MSP and CK	Daily	
410	will not be needed - <i>letter cancelled</i>		
411	Renewal - 20 day term - No response to renewal mailing	Monthly	
412	Renewal - Packet returned after due date - you must reapply	Daily	

Table 12: Eligibility Operations – CoverKids

CoverKids Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
CK100	CoverKids - Approval with effective dates	Daily	
CK101	CoverKids - Approval for maternity only for mother and child with effective date	Daily	
CK102a	CoverKids - Information is needed - SSN	Daily	
CK102b	CoverKids - Information is needed - proof your other coverage does not cover pregnancy care (maternity benefits)	Daily	
CK102c	CoverKids - Information is needed - date of birth	Daily	
CK102d	CoverKids - Information is needed - sign the application	Daily	
CK102e	CoverKids - Information is needed - provide proof you live in Tennessee	Daily	
CK102f	CoverKids - Information is needed - provide proof you have a verified American Indian/Alaska Native status	Daily	
CK103	CoverKids - Denial - new application	Daily	
CK104	CoverKids - Termination - coverage will end in 20 days	Daily	
CK105	CoverKids - Voluntary Termination - request received to end CK coverage	Daily	
CK106	CoverKids - Coverage was ended due to receipt of Date Of Death	Daily	
CK107	CoverKids - Reminder - inform CK of baby's name and DOB	Daily	
CK108	CoverKids - You informed us of a demographic change	Daily	
CK109	CoverKids - Application was received - you already have TennCare, on this effective date	Daily	

CoverKids Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
CK110	CoverKids - Please apply for CK on Health Insurance Marketplace	Daily	
CKSpec1	CoverKids- After denial, given second chance to complete renewal packet	Daily	

Table 13: Eligibility Operations – TEAMS

TEAMS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
ELG 301d	DENIAL - insufficient evidence of citizenship.	Daily	
ELG 301d	DENIAL - insufficient evidence of citizenship.	Daily	
AP 1	A hearing has been scheduled - phone - date and time.	Daily	
ELG.AI.cit	Additional Information needed to prove citizenship.	Daily	
ELG.AI.cit	Additional Information needed to prove citizenship.	Daily	
AP NOH.ph.5	Delay appeal - general delay in processing of application.	Daily	
AP AI.10cit	Delay appeal - additional information needed to prove citizenship - 10 days to respond.	Daily	
AP AI.90cit	CLOSING delay appeal - no response to request for proof of citizenship/immigrant eligibility - temporary TennCare APPROVED for 90 days.	Daily	
AP AI.combo	Delay appeal - additional information needed to prove income and citizenship - 10 days to respond.	Daily	
AP AI.in	Delay appeal - additional information needed to prove income - 10 days to respond.	Daily	
AP AI.MAGI	Delay appeal - additional information needed - haven't received info from the Marketplace - complete attached TennCare Delayed Application - 10 days to respond.	Daily	
AP AI.PrApp.2	Delay appeal - additional information needed to prove applied for TennCare - 10 days to respond.	Daily	
E-U - AD	CLOSING delay appeal - a TennCare application decision has been made - will get a letter about that decision.	Daily	
AP approved	CLOSING delay appeal - TennCare application has been approved.	Daily	
AP CI.App	CLOSING delay appeal - a TennCare application decision has been made - will get a letter with further information.	Daily	
AP CI.no delay.2	CLOSING delay appeal - no delay detected - TennCare application sent to Eligibility.	Daily	
AP CI.NoPrApp	Delay appeal CLOSED - no proof of date of application.	Daily	
AP D.cit	DENIAL/Delay appeal CLOSED/OPTIONAL CoverKids APPROVAL - no proof of citizenship.	Daily	
AP D.ftp	DENIAL/Delay appeal CLOSED - failure to provide additional information.	Daily	
AP D.in.3	DENIAL/Delay appeal CLOSED/OPTIONAL CoverKids APPROVAL - income too high.	Daily	

TEAMS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
AP D.ng	DENIAL/Delay appeal CLOSED - not in a group that Medicaid covers.	Daily	
AP D.nonres	DENIAL/Delay appeal CLOSED - non Tennessee resident <b>OR</b> receiving Medicaid in another state.	Daily	
AP D.prevcit	DENIAL/Delay appeal CLOSED/OPTIONAL CoverKids APPROVAL - not a US Citizen or eligible immigrant.	Daily	
AP IR	CLOSING Delay appeal - already have TennCare.	Daily	
AP Late.ver	Delay appeal is still CLOSED - appeal closed after no response to request for additional information - facts received after appeal closed - appeal still closed - facts sent to Eligibility staff - will get a letter about their decision.	Daily	
EAU.NP Closure	CLOSING request for hearing - no response to Request for Proof of Application.	Daily	
AP NOH.ph.4	Delay appeal - general delay in processing of application.	Daily	
	FORM "Request for Application Processing Delay Hearing"	Daily	
EAU.Untimely Closure	Cannot process request for hearing - no response to "Request for Application Processing Delay Hearing."	Daily	
AP res.app	CLOSING Delay appeal - TennCare application was already denied (can appeal denial).	Daily	
AP NOH.4	NOH - phone - delay appeal - appellant application for TennCare outstanding for 45 days or longer.	Daily	
Final Order.	Final Order.	Daily	
Order of Remand.	Order of Remand.	Daily	
Res IR.appeal	Denial appeal is CLOSED - already have TennCare.	Daily	
Auth R-p - individual	FORM "...Authorization of Individual Representative."	Daily	
Auth R-p - Organization	FORM "...Authorization of Representative Organization."	Daily	
EAU.AppDC	CLOSING delay appeal - already have TennCare.	Daily	
Initial Order rendered by an Administrative Judge.	Initial Order rendered by an Administrative Judge.	Daily	
Cover Pa“e	"See important information from TennCare on the next page of this letter."	Daily	
FIN.DEN NOH.ph	NOH - phone - application denial - appellant does not meet financial requirements for any open category of TennCare.	Daily	
Denial NOH.2	NOH - in person - application denial - appellant does not meet requirements for any group eligible for requested benefits.	Daily	
Denial NOH.2	NOH - phone - application denial - appellant does not meet requirements for any group eligible for requested benefits.	Daily	

TEAMS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
GEN.DEN NOH.ph	NOH - phone - application denial - appellant does not meet requirements for any open TennCare Medicaid category.	Daily	
TECH.DEN NOH.ph	NOH - phone - application denial - appellant does not fall within any open category of TennCare eligibility.	Daily	
ELG 301b	DENIAL - not in a group that Medicaid covers.	Daily	
ELG 301c	DENIAL - did not send the information needed to decide if you qualify.	Daily	
ELG 301a	DENIAL - recorded monthly income is over the income limit for Medicaid.	Daily	
EAU.DHS Cont.2	Appeal will be processed by DHS.	Daily	
EAU.effAck	Send proof of the date applied for TennCare.	Daily	
EFFDATE NOH.ph	NOH - phone - effective date - appellant requests an effective date of ____.	Daily	
Effdate res	APPROVED requested effective date - hearing no longer necessary.	Daily	
Effdate res.2	APPROVED requested effective date - hearing no longer necessary.	Daily	
Effdate NOH.3	NOH - in person - effective date appeal - appellant requests an effective date of ____.	Daily	
Effdate NOH.3	NOH - phone - effective date appeal - appellant requests an effective date of ____.	Daily	
ELG.Ala.dh	Before we set up a hearing we need to know more about household income.	Daily	
	Initial Order	Daily	
VFD.in.2	Hearing DENIED - did not tell us about a mistake that might qualify you for Medicaid.	Daily	
AP 2	Receipt of Motion	Daily	
AP 3	Receipt of Petition	Daily	
OIAI.1	After appeal/hearing/Judge's Order - additional information needed - 10 days to respond.	Daily	
OIU AI.90cit	After appeal/hearing/Judge's Order - no response to request for additional information needed - temporary TennCare APPROVED for 90 days.	Daily	
OIU AI.combo	After appeal/hearing/Judge's Order - additional information needed about household income and citizenship/immigration status - 10 days to respond.	Daily	
OIU AI.in	After appeal/hearing/Judge's Order - additional information needed about household income - 10 days to respond.	Daily	
OIU AI.res	After appeal/hearing/Judge's Order - additional information needed about Tennessee state residency - 10 days to respond.	Daily	
OIU AI.resubmit	After appeal/hearing/Judge's Order - please RESUBMIT additional information sent - 10 days to respond.	Daily	
OIU AI.ssn	After appeal/hearing/Judge's Order - additional information needed of SSN - 10 days to respond.	Daily	
OIU D.ftp	After appeal/hearing/Judge's Order - application DENIED - appeal CLOSED - no response to request for additional information.	Daily	
OIU D.in	After appeal/hearing/Judge's Order - application DENIED - appeal	Daily	

TEAMS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
	CLOSED/OPTIONAL CoverKids APPROVAL - income too high.		
OIU D.ng	After appeal/hearing/Judge's Order - application DENIED - appeal CLOSED - not in a group that Medicaid covers.	Daily	
OIU D.res	After appeal/hearing/Judge's Order - application DENIED - appeal CLOSED - not TN resident <b>OR</b> receiving Medicaid from another state.	Daily	
OIU D.prevcit	After appeal/hearing/Judge's Order - application DENIED - appeal CLOSED/OPTIONAL CoverKids APPROVAL - non citizen or eligible immigrant.	Daily	
OIU IR	After appeal/hearing/Judge's Order - already have TennCare.	Daily	
OIU Order.gen	After appeal/hearing - here is the Judge's Order...	Daily	
Initial Order for continuance of appeal	Initial Order for continuance of appeal	Daily	
Order for withdrawal of appeal	Order for withdrawal of appeal	Daily	
Order	Order	Daily	
Notice of receipt of petition for APPEAL of Initial Order.	Notice of receipt of petition for APPEAL of Initial Order.	Daily	
Reconsideration Order	Reconsideration Order	Daily	
Order of Remand.	Order of Remand.	Daily	
Refer to SSA	Delay appeal CLOSED - SSI recipient - SSA decides start date.	Daily	
Res.approve.1	We agree with your appeal - call if you still want a hearing.	Daily	
GEN.TERM NOH.ph	NOH - phone - termination.	Daily	
Untimely Close.den.2	CLOSING denial appeal - too late to appeal/after 40 day appeal period.	Daily	
Untimely Close.effdate.2	CLOSING effective date appeal - too late to appeal/after 40 day appeal period.	Daily	
Accepted.1	Hearing APPROVED - phone.	Daily	
Denied.1	Hearing DENIED - appeal CLOSED - didn't give facts needed.	Daily	
VFD.in.3	Hearing DENIED - did not tell us about a mistake that might qualify you for Medicaid.	Daily	
VFD.in.4	Hearing DENIED - did not tell us about a mistake that might qualify you for Medicaid.	Daily	
WD.Closure.1	Withdrawal form received - CLOSING appeal.	Daily	
Withdrawal form	FORM "How to end your TennCare appeal."	Daily	

TEAMS Letter ID	Description (Policy – Letter Title)	Current or Planned Frequency	Monthly Volume (Where Applicable)
WD.Closure.1	Withdrawal form received - CLOSING appeal.	Daily	

## Contract ATTACHMENT 4

**LETTER OF DIVERSITY COMMITMENT****SAMPLE LETTER OF DIVERSITY COMMITMENT****(Company Letterhead/Logo)****(Address)****(Date)****(Salutation),**

**(Company Name)** is committed to achieving or surpassing a goal of **(numeral)** percent spend with certified diversity business enterprise firms on State of Tennessee contract # **(Edison document #)**. Diversity businesses are defined as those that are owned by minority, women, small business and Tennessee service-disabled veterans which are certified by the Governor's Office of Diversity Business Enterprise (Go-DBE).

We confirm our commitment of **(percentage)** participation on the **(Contract)** by using the following diversity businesses:

- (i) Name and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veteran) of anticipated diversity subcontractors and suppliers:  
\_\_\_\_\_
- (ii) Participation estimates (expressed as a percent of the total contract value to be dedicated to diversity subcontractors and suppliers):  
\_\_\_\_\_%)
- (iii) Description of anticipated services to be performed by diversity subcontractors and suppliers:  
\_\_\_\_\_  
\_\_\_\_\_

We accept that our commitment to diversity advances the State's efforts to expand opportunity of diversity businesses to do business with the State as contractors and sub-contractors.

Further, we commit to:

1. Using applicable reporting tools that allow the State to track and report purchases from businesses owned by minority, women, Tennessee service-disabled veterans and small business.

Reporting quarterly to the Go-DBE office the dollars spent with certified diversity businesses owned by minority, women, Tennessee service-disabled veterans and small business accomplished under contract # (Edison number

2. ).

(Company Name) is committed to working with the Go-DBE office to accomplish this goal.

Regards,

(Company authority – signature and title)

## Contract ATTACHMENT 5

**LIST OF INTERFACES**

The following is a list of Eligibility Operations Interfaces that shall be utilized by the State of Tennessee for the TEDS:

*Table 14: Eligibility Operations Interfaces*

Source	Source Association	Common File Name	In/Out	Frequency	Destination	Notes
FDSH	CMS	H03 SSA Composite	In	On Demand	TEDS	
FDSH	CMS	H08T Verify Current Income	In	On Demand	TEDS	
FDSH	CMS	H09T Verify Annual Household Income	In	On Demand	TEDS	
FDSH	CMS	H59 Verify Lawful Presence	In	On Demand	TEDS	
FDSH	CMS	H61 VLP Closed Case	In	On Demand	TEDS	
FDSH	CMS	H15 Account Transfer	In	Daily	TEDS	
TMED	TennCare	TMED	In	On Demand	TEDS	
TEDS	TennCare	H15 Account Transfer	Out	Daily	FDSH	
TEDS	TennCare	Inbound Eligibility Interface File	Out	Daily (every business day, Monday - Friday)	TSMIS	TEDS to interChange Eligibility Interface File
TEDS	TennCare	Inbound Linking Interface File	Out	Daily (every business day, Monday - Friday)	TSMIS	Linking file from TEDS that shall be used to link recipients together
TCMIS	TennCare	Eligibility/Demographic Error File	In	Daily (every business day, Monday - Friday)	TEDS	After interChange processes the daily TEDS Eligibility/Demographic File, an error response file shall be generated and sent to TEDS containing all processing errors
TCMIS	TennCare	Linking Error File	In	Daily (every business day, Monday - Friday)	TEDS	After interChange processes the daily TEDS Linking file, an error response file shall be generated and sent to TEDS

Source	Source Association	Common File Name	In/Out	Frequency	Destination	Notes
						containing all processing errors.
TCMIS	TennCare	Run-Out File Containing Demographics and Address (InterChange to TEDS Outbound)	In	Daily	TEDS	An interface between TEDS and interChange for Accent data during the Run out Period
TCMIS	TennCare	Run-Out File Containing Recipient Eligibility (InterChange to TEDS Outbound)	In	Daily	TEDS	An interface between TEDS and interChange for Accent data during the Run out Period
TCMIS	TennCare	MCO Reported Address	In	Weekly	TEDS	To Update MCO Reported address from MMIS system to TEDS.
TCMIS	TennCare	TPL File	In	Monthly	TEDS	To Update MCO Reported address from MMIS system to TEDS.
TCMIS	TennCare	ME Encounter File	In	Monthly	TEDS	To Update ME Encounter data from MMIS system to TEDS.
TCMIS	TennCare	Priority Population File	In	Monthly	TEDS	To Update Priority Population (PP) data from MMIS system to TEDS.
TCMIS	TennCare	NPI Provider File	In	Monthly	TEDS	To Update Priority Population (PP) data from MMIS system to TEDS.
FDSH	CMS	H31 Verify Non-Employer Sponsored Insurance Minimal Essential Coverage (Non-ESI MEC)	In	On Demand	TEDS	
DHS	SSA	SDX	In	Daily and Monthly	TEDS	
DHS	SSA	BEERS	In	Daily	TEDS	
DHS	SSA	Low Income Subsidy(LIS)	In	Daily	TEDS	
TALX	NHI	Employment and Income Verification Systems (TALX)	In	On Demand	TEDS	TALX will provide employment and salary information upon request by TEDS. TEDS will interface with the

Source	Source Association	Common File Name	In/Out	Frequency	Destination	Notes
						Equifax/TALX Work Number system. The Work Number provides employment and salary information
<b>DOL</b>	DOL	Wage, New Hire and UI	In	Quarterly	TEDS	TEDS will receive quarterly wages, new hire, and unemployment information from the Tennessee Department of Labor and Workforce.
<b>DOH</b>	DOH	Vital Statistics	In	Monthly	TEDS	
<b>Correction</b>	DOC	Prisoner File	In	Three times a year	TEDS	
<b>TennCare</b>	TEDS	DIFSLA	Out	Yearly	IRS	TEDS will send eligibility data about cases to the IRS through the Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) interface. This process will send updates on a yearly basis
<b>IRS</b>	IRS	Federal Tax Information (FTI)	In	Yearly	TEDS	This interface will allow TEDS to receive, store and process tax information between itself and the FTI.
<b>TennCare</b>	TEDS	State Verification Exchange (SVES)	Out	Daily	SSA	
<b>TennCare</b>	TEDS	Supplementary Medical Insurance (SMI) Buy-In(s)	Out	Monthly	CMS	
<b>CMS</b>	CMS	Supplementary Medical Insurance (SMI) Buy-In(s)	In	Monthly	TEDS	
<b>PARIS</b>	ACF	Public Assistance Reporting Information System (PARIS)	In	Quarterly	TEDS	
<b>PARIS</b>	ACF	Public Assistance Reporting Information System (PARIS)	Out	Quarterly	ACF	

Source	Source Association	Common File Name	In/Out	Frequency	Destination	Notes
<b>Tennessee Department of Finance, Benefits and Administration</b>	Tennessee Department of Finance, Benefits and Administration	TISS Report	In		TEDS	This interface will allow TEDS to receive and process state employment information
<b>EVVE</b>	NAPHSIS	Electronic Verification of Vital Events (EVVE)	In	On Demand	TEDS	TEDS will interface with the National Association for Public Health Statistics and Information Services' (NAPHSIS) Electronic Verification of Vital Events (EVVE) system to allow immediate confirmation of the information on a birth certificate presented by an applicant

## Contract ATTACHMENT 6

**LIST OF REPORTS**

The following is a list of Eligibility Operations Reports that are currently generated by the State of Tennessee:

*Table 15: Eligibility Operations Reports*

<b>Report Name</b>	<b>Type</b>
Active Individuals by Program Report	State
BCC Treatment Plan Report	State
Deceased Report	State
Daily Error Detail Report	State
Daily Error Summary Report	State
Pseudo SSN Report	State
Pending Re-verification Report	State
QI Eligible Individuals Report	State
Application Aging Report	State
Low Income Subsidy (LIS) Report	State
LTSS Recipients With Trusts or Annuities Report	State
Applications Disposed with a Time Frame Report	State
Cost of Living Adjustment Report	State
Applications Report	State
Denials Report	State
Redetermination Report	State
MGMT 2050 Supervisory Report	State
DCS Foster Care and Adoption Assistance Redetermination Report	State
Foster Care and Adoption Assistance Pending Applications Report	State
Error Reports from Mass Change Processing	State
Active Case Report	State/Federal
Application Processed Report	State/Federal
Eligibility Determination Reports	State/Federal
Application Status and Duration	State
Number of Applications Received Through Various Channels	State/Federal
Cases Approaching Timeliness Deadline Report	State
Due and Past Due Case Report	State
Processing Time by Application Date Report	State/Federal
Processing Time by Receipt Date Report	State/Federal
Case Load Report	State
Report on the Amount of Active cases/Tasks assigned to a Unit, and Worker	State
Program Enrollment Forecast	State
Appeal Activity Report	State
Appeals Summary Report	State
KPI Reports	State
Appeal Docket	State
Appeal Dashboard	State
Appeal Case Status Report	State
Appeals Summary Report	State
CHIP Report	State

## DEFINITIONS AND ABBREVIATIONS

*Table 16: Abbreviations*

<b>Abbreviation</b>	<b>Definition</b>
<b>24/7/365</b>	Available twenty-four (24) hours per day, seven (7) days per week, and three hundred sixty-five (365) days per year
<b>ACCENT</b>	Automated Client Certification and Eligibility Network for Tennessee
<b>ACF</b>	Administration for Children and Families
<b>ACH</b>	Automated Clearing House
<b>AOA</b>	Annual Operational Assessment
<b>ATC</b>	Authority to Connect
<b>ATO</b>	Authority to Operate
<b>ATP</b>	Account Transfer Process
<b>BABOK</b>	Business Analysis Body of Knowledge
<b>BC/DR</b>	Business Continuity and Disaster Recovery
<b>BIA</b>	Business Impact Analysis
<b>BOM</b>	Business Operating Model
<b>BPM</b>	Business Process Management
<b>BRD</b>	Business Requirements Document
<b>BRE</b>	Business Rules Engine
<b>BRMS</b>	Business Rules Management System
<b>CAP</b>	Corrective Action Plan
<b>CD</b>	Control Directive
<b>CFR</b>	Code of Federal Regulations
<b>CHIP</b>	Children's Health Insurance Program
<b>CI</b>	Configuration Item
<b>CIO</b>	Chief Information Officer
<b>CIP</b>	Continuous Improvement Process
<b>CISM</b>	Certified Information Security Manager
<b>CISSP</b>	Certified Information Systems Security Professional
<b>CM</b>	Control Memorandum
<b>CMDB</b>	Configuration Management Database
<b>CMPPA</b>	Computer Matching and Privacy Protection Act of 1988
<b>CMS</b>	Centers for Medicare and Medicaid Services
<b>COTS</b>	Commercial Off-the-Shelf
<b>CP</b>	Contingency Plan
<b>CPO</b>	Chief Privacy Officer
<b>DAC</b>	Disabled Adult Child
<b>DB</b>	Database
<b>DBMS</b>	Database Management System
<b>DCS</b>	Department of Children's Services
<b>DDI</b>	Design, Development, and Implementation
<b>DED</b>	Deliverable Expectations Document
<b>DHS</b>	Department of Human Services (State of Tennessee)
<b>DIFSLA</b>	Disclosure of Information to Federal, State, and Local Agencies

<b>Abbreviation</b>	<b>Definition</b>
<b>DNS</b>	Domain Name System
<b>DOH</b>	Department of Health
<b>DOJ</b>	Department of Justice
<b>DOLWD</b>	Department of Labor and Workforce Development
<b>DUNS</b>	Data Universal Numbering System
<b>EA</b>	Enterprise Architecture
<b>ECM</b>	Electronic Content Management
<b>ED</b>	Eligibility Determination
<b>ELC</b>	Enterprise Life Cycle
<b>EMP</b>	Eligibility Modernization Project
<b>EMPPA</b>	Eligibility Modernization Project Process Agreement
<b>EOG</b>	Eligibility Operations Group
<b>ERR</b>	Environment Readiness Review
<b>ESB</b>	Enterprise Service Bus
<b>ESM</b>	Enterprise System Modernization
<b>ETL</b>	Extract, Transform, and Load
<b>EVVE</b>	Electronic Verification of Vital Events
<b>FDSH</b>	Federal Data Services Hub
<b>FEIN</b>	Federal Employer Identification Number
<b>FFATA</b>	Federal Funding Accountability and Transparency Act
<b>FFM</b>	Federally Facilitated Marketplace
<b>FTE</b>	Full-time Equivalent
<b>FTI</b>	Federal Tax Information
<b>GIAC</b>	Global Information Assurance Certification
<b>GLBA</b>	Graham-Leach-Bliley Act of 1999
<b>Go-DBE</b>	Governor's Office of Diversity Business Enterprise
<b>GUI</b>	Graphical User Interface
<b>HCFA</b>	Division of Health Care Finance and Administration (State of Tennessee)
<b>HHS</b>	U.S. Department of Health and Human Services
<b>HIPAA</b>	Health Insurance Portability and Accountability Act of 1996
<b>HITECH</b>	Health Information Technology for Economic and Clinical Health Act
<b>ICD</b>	Interface Control Document
<b>IEA</b>	Information Exchange Agreement
<b>IMS</b>	Integrated Master Schedule
<b>IRC</b>	Internal Revenue Code
<b>IRR</b>	Implementation Readiness Review
<b>IRS</b>	Internal Revenue Service
<b>IS</b>	Information Systems
<b>ISA</b>	Interconnected Systems Agreement
<b>IT</b>	Information Technology
<b>ITIL</b>	Information Technology Infrastructure Library
<b>IV&amp;V</b>	Independent Verification and Validation
<b>KPI</b>	Key Performance Indicator
<b>LAN</b>	Local Area Network
<b>LD</b>	Liquidated Damage
<b>LIS</b>	Low Income Subsidy
<b>LTSS</b>	Long Term Services and Supports

<b>Abbreviation</b>	<b>Definition</b>
<b>O&amp;M</b>	Operations and Maintenance
<b>MAGI</b>	Modified Adjusted Gross Income
<b>MARS-E</b>	Minimum Acceptable Risk Standards for Exchanges
<b>MCO</b>	Managed Care Organization
<b>ME</b>	Medically Eligible
<b>MFA</b>	Multi-Factor Authentication
<b>MITA</b>	Medicaid Information Technology Architecture
<b>MMIS</b>	Medicaid Management Information System
<b>MMP</b>	Medicaid Modernization Program
<b>MOU</b>	Memorandum of Understanding
<b>MPI</b>	Master Person Index
<b>MSP</b>	Medicare Savings Program
<b>NAPHSIS</b>	National Association for Public Health Statistics and Information Services
<b>NCPD</b>	Notice of Calculation of Potential Damages
<b>NIAD</b>	Notice of Intent to Assess Damages
<b>NIST</b>	National Institute of Standards and Technology
<b>NOC</b>	Network Operations Center
<b>NPD</b>	Notice of Potential Damages
<b>NTP</b>	Network Time Protocol
<b>OASDI</b>	Old Age, Survivor, and Disability Insurance
<b>OCMT</b>	Organizational Change Management and Training
<b>OMB</b>	Office of Management and Budget
<b>OS</b>	Operating System
<b>OSSTMM</b>	Open Source Security Testing Methodology Manual
<b>PARIS</b>	Public Assistance Reporting Information System
<b>PHI</b>	Protected Health Information
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>PMI</b>	Project Management Institute
<b>PMLC</b>	Project Management Lifecycle
<b>PMO</b>	Project Management Office
<b>PMP</b>	Project Management Plan
<b>POA&amp;M</b>	Plan of Actions and Milestones
<b>PP</b>	Priority Population
<b>PPACA</b>	Patient Protection and Affordable Care Act
<b>QA</b>	Quality Assurance
<b>QI</b>	Qualified Individuals
<b>QM</b>	Quality Management
<b>RA</b>	Risk Assessment
<b>RFC</b>	Request for Change
<b>RFQ</b>	Request for Qualifications
<b>RMF</b>	Risk Management Framework
<b>RPO</b>	Recovery Point Objective
<b>RTM</b>	Requirements Traceability Matrix
<b>RTO</b>	Recovery Time Objective
<b>SADD</b>	System Architecture Design Document
<b>SCA</b>	Security Control Assessment

<b>Abbreviation</b>	<b>Definition</b>
<b>SDLC</b>	System Development Lifecycle
<b>SDX</b>	State Data Exchange
<b>SFTP</b>	Secure File Transfer Protocol
<b>SI</b>	System Integration
<b>SIT</b>	System Integration Testing
<b>SLA</b>	Service Level Agreement
<b>SLR</b>	Service Level Requirement
<b>SME</b>	Subject Matter Expert
<b>SMI</b>	Supplementary Medical Insurance
<b>SNAP</b>	Supplemental Nutrition Assistance Program
<b>SOA</b>	Service Oriented Architecture
<b>SOAP</b>	Simple Object Access Protocol
<b>SOP</b>	Standard Operating Procedure
<b>SP</b>	Special Publication
<b>SPMO</b>	Strategic Program Management Office
<b>SQL</b>	Structured Query Language
<b>SSA</b>	United States Social Security Administration
<b>SSI</b>	Supplemental Security Income
<b>SSN</b>	Social Security Number
<b>SSO</b>	Systems Security Officer
<b>SSP</b>	System Security Plan
<b>SSR</b>	Safeguard Security Report
<b>ST&amp;E</b>	Security Test and Evaluation
<b>STS</b>	Strategic Technology Solutions
<b>TANF</b>	Temporary Assistance for Needy Families
<b>TARB</b>	Technical Architecture Review Board
<b>TAS</b>	Technical Advisory Services
<b>TCA</b>	Tennessee Code Annotated
<b>TCCB</b>	Technical Change Control Board
<b>TCMIS</b>	TennCare Management Information System
<b>TCRS</b>	Tennessee Consolidated Retirement System
<b>TEAMS</b>	Tennessee Eligibility Appeals Management System
<b>TEDS</b>	Tennessee Eligibility Determination System
<b>TMED</b>	Tennessee Medical Eligibility Determination System
<b>TNHC</b>	Tennessee Health Connection
<b>TOGAF</b>	The Open Group Architecture Forum
<b>TPL</b>	Third Party Liability
<b>UAT</b>	User Acceptance Testing
<b>USC</b>	United States Code
<b>USPS</b>	United States Postal Service
<b>VLP</b>	Verify Lawful Presence
<b>WAN</b>	Wide Area Network
<b>WBS</b>	Work Breakdown Structure
<b>WCAG</b>	Web Content Accessibility Guidelines
<b>WRS TN Tower</b>	William R. Snodgrass Tennessee Tower
<b>XML</b>	Extensible Markup Language

Table 17: Definitions

Term	Definition
<b>Accessibility Testing</b>	Accessibility Testing is to ensure that the product is compliant with applicable Section 508 Accessibility and WCAG 2.0 AA Standards identified in the completed Section 508 Product Assessment. Software products (whether COTS, Government Off-the-Shelf, or custom-developed software applications) must adhere to Section 508 accessibility and other regulatory requirements governing the use of EIT in accordance with the CMS Policy for Section 508 Compliance. Accessibility Testing is required if the business application has a user interface or produces electronic output for direct access or use by federal employees or the public.
<b>Account transfers</b>	Automated process to receive applications originally entered through the Federally Facilitated Marketplace.
<b>Ad-hoc Testing</b>	Testing performed without planning and documentation where the tester tries to 'break' the system by randomly trying the system's functionality. Ad-hoc testing is typically informal and improvisational.
<b>Alert/Monitoring Testing</b>	Alert/Monitoring Testing is the type of testing that is done where you purposely end test scenarios/cases in actions that would result in a system alert/message, ensuring that the correct actions are taken at that time. Alerts could be from a user perspective (telling the user that they provided the wrong SSN because it begins with 999), or on the system side (the system has received error code 01239, and the system knows how to handle that error code). Monitoring testing is that for known errors/messages, the system should be ready to monitor for those and intercept them and react to them appropriately.
<b>Beta Testing</b>	Beta testing of the Solution is run in a production environment and in parallel with the legacy production system. It allows a comparison of the results of processing between the legacy system and the new solution based on live data in the parallel production environments. It ensures that business sponsors are able to validate that the delivered solution in the target production environment supports all business requirements.
<b>Boundary Testing</b>	Boundary Testing consists of testing the extremes of the input domain, e.g. maximum, minimum, just inside/outside boundaries, typical values, and error values.
<b>Business Management Tool</b>	Repository based on a defined strategy, allowing the defined rules to be managed in terms of versions and variants. The Businesses Rules Management tool shall be available to all relevant stakeholders to define and manage the business rules.
<b>Communication Management</b>	A component of the Project, Program, or Portfolio Management that describes how, when and by whom information about the project will be administered and disseminated.
<b>Compatibility Testing</b>	Compatibility Testing validates how well a software performs in a particular hardware/software/operating system/network environment. Backward Compatibility Testing tests the application or software in old or previous versions. Forward Compatibility Testing tests the application or software in new or upcoming versions.
<b>Component Integration Testing</b>	Component Integration Testing validates that all software components interact with one another correctly.
<b>Configuration Management</b>	Configuration Management includes the process of documenting formal procedures to apply technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a product, result, service, or component; control any changes to such characteristics; record and report each change and its implementation status; and support the audit of the products, results or components to verify conformance to requirements. It includes the documentation, tracking systems, and defined approvals necessary for authorizing and controlling changes.
<b>Conversion Testing</b>	Conversion Testing is a testing process prescribed in the Data Conversion Plan that ensure testing is done in a manner reflective on how the system will be used in its "real" environment.
<b>Eligibility Modernization Project</b>	The Eligibility Modernization Project represent the State of Tennessee's highest priority in the Medicaid Modernization Program. The project's scope involves development and implementation of an eligibility determination system for TennCare and CHIP, which shall contain a rules-based decision engine, and that will be compliant with the Affordable Care Act, CMS requirements and all applicable State and Federal Regulations.
<b>Eligibility Modernization Project Process Agreement</b>	The Eligibility Modernization Project Process Agreement (EMPPA) is used to authorize and document the justifications for using, not using, or combining specific Gate Reviews and the selection of specific deliverables applicable to the investment of Eligibility Modernization Project, including the expected level of detail to be provided. This document authorizes the project to

Term	Definition
	proceed according to agreed upon scope, time, costs, and quality including any related exceptions as outlined within this document.
<b>Eligibility Modernization Project Steering Committee</b>	Members of the Eligibility Modernization Project Steering Committee shall be defined by the State.
<b>End-to-End Testing</b>	End-to-End Testing tests all of the business application's access or touch points, and data, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure business processes are successfully completed. Testing will be conducted on a complete, integrated set of business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly.
<b>Enterprise Testing</b>	Enterprise Testing tests all enterprise business applications that may have direct or indirect touch-points across multiple business applications and systems. Testing will be conducted on a complete, integrated set of enterprise business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly.
<b>Environment Readiness Review</b>	The Environment Readiness Review is a representation of the Validation Readiness Review, Implementation Readiness Review, and Production Readiness Review. These reviews are needed to enter the various CMS environments to test the solution and its contingency operations. Not all solutions will go through all environments. Specific requirements for running in each environment are provided by the environment's owner.
<b>Error Handling Testing</b>	Assesses the ability of the system to properly process erroneous transactions. The main objectives are to ensure that all reasonably anticipated error conditions are recognizable by the application system, accountability for processing errors has been assigned and that the procedures provide a high probability that the error will be properly corrected, and that reasonable control is maintained over errors during the correction process.
<b>Exploratory Testing</b>	Emphasizes the personal freedom and responsibility of the individual tester to continually optimize the quality of his/her work by treating test-related learning, test design, test execution, and test result interpretation as mutually supportive activities that run in parallel throughout the project.
<b>Failover Clustering</b>	Failover Clustering is a failsafe in which a two or more servers work together to ensure that if one (or more) fail, that another can seamlessly take over the workload without any downtime.
<b>Federal Facilitated Marketplace</b>	A CMS system providing consumer and small business access to a health insurance marketplace for states that have chosen not to build their own marketplace.
<b>Financial Management</b>	Financial Management is a process which brings together planning, budgeting, accounting, financial reporting, internal control, auditing, procurement, disbursement and the physical performance of the project with the aim of managing project resources properly and achieving the project's objectives. Like the concept of Project Management, it is a strategic competency for organizations and can make the difference between a successful project and audit reports.
<b>Functional Requirement</b>	Functional requirements define the expected functionality of the product or Solution to be created.
<b>Functional Testing</b>	Assess the input/output functions of a business application against pre-defined functional and data requirements. Each and every functionality of the system is tested by providing appropriate input, verifying the output and comparing the actual results with the expected results. Types of functional testing include: Unit Testing, Smoke Testing, Sanity Testing, Integration Testing, White Box Testing, Black Box Testing, User Acceptance testing, Regression Testing
<b>Gate Review</b>	A Gate Review is a phase-driven go/no-go decision point where project activities are reviewed to assure that appropriate requirements are observed. A project cannot proceed without a Go decision by the appropriate senior management for a specific stage gate. Each Gate Review is an independent confirmation by the Gate Review Team (including relevant critical partners) to the IT Governance organization or delegated authority that all required project reviews have been successfully conducted. It checks that the EMP Manager has satisfactorily produced all the required deliverables and met all exit criteria for a given SDLC phase to permit advancement to the next phase.

Term	Definition
	<p>The emphasis of the Gate Review is on:</p> <ul style="list-style-type: none"> <li>a) The successful accomplishment of SDLC phase objectives;</li> <li>b) The plans for the next life cycle phase; and</li> <li>c) The risks associated with moving into the next life cycle phase.</li> </ul> <p>The results of the Gate Review Team's assessment are provided with recommended action to the IT Governance organization or delegated authority for decision.</p>
<b>Go-Live</b>	Successful implementation and deployment of all functionality aligned with a Release to the end-user population.
<b>Go/No-Go Decision</b>	Point at which a decision to continue or stop a course of action is made. If a decision is made to "go", this denotes that the solution conforms to the documented specifications.
<b>GUI Navigation Testing</b>	Validates the system logic behind when a user navigates from one screen to another. In a GUI system, at each time frame there is an active screen interacting with the user. The active screen, when triggered by specific event, will disappear or be deactivated and another one will be loaded in or activated. The two screens are logically connected by the event and such a scenario where the screen focus is shifted is called screen navigation.
<b>GUI Software Testing</b>	Testing through the use of a GUI, to ensure it meets agreed upon specifications as defined prior to software development. GUI testing evaluates design elements such as layout, colors, fonts, font sizes, labels, text boxes, text formatting, captions, buttons, lists, icons, links, and content.
<b>Human Resources Management</b>	A component of the Project Management Plan that describes how the roles and responsibilities, reporting relationships, and staff management will be addressed and structured.
<b>Implementation Readiness Review</b>	Gate Review to ensure the solution completed through Integration Testing and is ready for turnover to the formal, controlled test environment for Production Readiness.
<b>Interface Testing</b>	Interface Testing tests all of the business application's access or touch points, and data, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure business processes are successfully completed. Testing will be conducted on a complete, integrated set of business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly. This testing function is sometimes referred to as End-to-End Integration Testing.
<b>IV&amp;V Attestation</b>	IV&V Attestation is the process of establishing documented evidence that the solution does what it has been designed to do and will continue to operate correctly in the future. IV&V Attestation provides objective evidence that all software requirements have been implemented correctly and completely. This includes evidence that the solution produces the intended results and that all functionality is traceable to solution requirements.
<b>MARS-E</b>	A document suite of guidance, requirements, and templates assembled by CMS. The document suite contains implementation standards for key security requirements contained in Department of Health and Human Services (HHS) ACA Regulations (45 CFR §§155.260 and 155.280) and other State and Federal regulations and policies. This is a harmonized set of guidelines inclusive of CMS and IRS requirements. Any reference to this package, even under CMS context references, should also infer compliance with current IRS Safeguards Program and IRS Pub 1075 where applicable by usage of data type and/or classification.
<b>Medicaid Modernization Program</b>	Medicaid Modernization Program is comprised of multiple sub-projects and is an initiative by the State of Tennessee to improve health care quality and access for members, achieve greater accountability for outcomes, create a more predictable and sustainable Medicaid budget, achieve more flexibility and scalability to meet the future needs of TennCare and CHIP program.
<b>Member Matching</b>	Determination if any given individual is a current Medicaid member (if they have a current Medicaid Plan)
<b>Member Portal</b>	The Member Portal shall provide Solution access to applicable insurance plan members or applicants.
<b>Negative Testing</b>	A Negative test will assess the response of the system outside of normal parameters and is designed to assess the system's ability to successfully perform error handling with the unexpected input. The tester uses invalid inputs or imitates unexpected user behavior to expose potential errors and system risk.
<b>Non-Functional</b>	Non-functional Requirements define the specific technical functionality that must exist in the

<b>Term</b>	<b>Definition</b>
<b>Requirement</b>	Solution to deliver the business functionality, the operational objectives of the Solution, and the methodology and processes to manage the Solution delivery.
<b>Operational Readiness Testing</b>	Ensure that the operational readiness is appropriately comprehensive and inclusive of all elements of the State enterprise impacted by the TEDS deployment. Operational readiness may include checking the backup/restore facilities, IT disaster recovery procedures, maintenance tasks, and periodic check of security vulnerabilities.
<b>Partner Portal</b>	The Partner Portal shall provide Solution access to current TennCare Pre-Admission Evaluation System users, nursing homes, and hospitals. The Partner Portal shall be accessible both within the State of Tennessee network, and outside of the State of Tennessee network.
<b>Performance Management</b>	Performance Management is the use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet those goals, and report on the success in meeting those goals.
<b>Performance Testing</b>	Assesses the capacity and throughput of a business application and/or infrastructure in processing time, CPU utilization, network utilization, and memory and storage capacities relative to expected normal (average and peak) user and processing load as defined in the system's requirements document and/or Operation Manual document.
<b>Production Instance</b>	Denotes the version of the code that is in operation.
<b>Quality Control Testing</b>	Testing that determines if the system is performing and adheres to the predetermined requirements and expectations. The testing will verify the system was developed as outlined in the documented requirements.
<b>Quality Management</b>	Quality Management includes the process and activities of performing organization that determine quality policies, objectives, and responsibilities so that the project will satisfy the needs for which it was undertaken. Quality Management uses policies and procedures to implement, within the project's context, the organization's quality management system and, as appropriate, it supports continuous process improvement activities as undertaken on behalf of the performing organization. Quality Management works to ensure that the project requirements, including product requirements are met and validated.
<b>Release</b>	A Release is the distribution of the updated version of the solution. Release can be a stage in development of a solution or maturity for a piece of software: ranging from its initial development to its eventual release, and including updated versions of the released version to help improve software or fix bugs still present in the solution.
<b>Recovery Testing</b>	Validates how well an application is able to recover from crashes, hardware failures, and other similar problems. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
<b>Regression Testing</b>	Selective re-testing to validate that modifications have not caused unintended functional or data results and that the application still complies with its specific requirements.
<b>Reliability Testing</b>	Monitor the operational availability of business applications and/or infrastructure, problems/incidents, performance/service level, and capacity utilization of production systems, and will validate the gathered data against expected results (documented in the system's requirement document and/or Operation Manual document) to ensure that the implemented application or infrastructure performs as expected in production. This testing function is sometimes referred to as Reliability Validation, Burn in Period, Reliability Test, or Extended Reliability Test.
<b>Requirements Management Tool</b>	Repository based on a defined strategy, identifying the relationship, interface, or dependency on data in other tools. A Requirements Management tool will describe how the traceability strategy and how the requirements will be structured.
<b>Requirements Traceability Matrix</b>	A grid that links product requirements from their origin to the deliverables that satisfy them. The implementation of Requirements Traceability Matrix helps ensure that each requirement adds business value by linking it to the business and project objectives. It provides a means to track requirements throughout the project lifecycle, helping to ensure that requirements approved in the requirements documentation are delivered at the end of the project. Finally, it provides a structure for managing changes to the scope.
<b>Risk and Issue Escalation</b>	Process of identifying time frames and the management chains (names) for escalation of issues and risks that cannot be resolved at a lower staff level.
<b>Risk</b>	Framework required by the State of Tennessee to inform, advise, and manage the activities of

Term	Definition
<b>Management Framework (RMF)</b>	security categorization (as defined in the federal publication FIPS 199), security control selection and implementation, security control assessment, information system authorization (ATO and ATC), and security control monitoring. The State must approve the RMF and it must meet standard practices associated with effective implementation, management, and maintenance of the NIST RMF.
<b>Scalability Testing</b>	Identify major workloads and mitigate bottlenecks that can impede the scalability of the application. Scalability testing is a subset of performance testing. Performance testing can be used to establish a baseline against which future performance tests can be compared against.
<b>Schedule Management</b>	Schedule Management is a subsidiary of, and integrated with, the Project Management. Schedule Management identifies a scheduling method and scheduling tool and sets the format and establishes criteria for developing and controlling the project schedule. The selected scheduling method defines the framework and algorithms used in the scheduling tool to create the schedule model. Some of the better known scheduling methods include Critical Path Method and Critical Chain Method.
<b>Scope Management</b>	Scope Management is a discipline of Project Management that defines how the project scope will be defined, validated and controlled. The key benefit of the process is that it provides guidance on how scope will be managed throughout the project.
<b>Security and Privacy Controls</b>	<p>The security and privacy controls that apply to information assets, in principal, are commensurate with the potential impact on information assets, organizational operations, or individuals, should there be a compromise of confidentiality, integrity, or availability of the information. Federal and State regulations and policies define specific classifications of data that require specific levels of control. In some instances, such as FTI, the source of the data is a factor in determining the security and privacy controls that apply to data elements. Security and privacy controls shall include, at a minimum:</p> <ul style="list-style-type: none"> <li>a) Role based access</li> <li>b) Data ownership/authorization rights</li> <li>c) MFA - when a third party accesses sensitive information about another person</li> <li>d) Encryption of information in transit</li> <li>e) Encryption of information at rest</li> <li>f) Data masking/synthetic data requirements</li> <li>g) Secure file transfers</li> <li>h) Masking of data elements on displays or reports (for example, replacing all but the last four digits of a key person identifier such as an SSN)</li> <li>i) Recording an audit trail of who accesses what specific sensitive data and when Training</li> </ul> <p>Classification of the data, with respect to sensitivity of content and source governance, drives the security and privacy controls for the data. This is a key activity that shall be completed to the approval of the State Chief Security Officer, Chief Privacy Officer (CPO), and other stakeholders at project initiation. This classification serves as the foundation for security activities throughout the SDLC.</p>
<b>Security and Privacy Management Tools</b>	<p>The State requires management of security and privacy in compliance with Federal and State regulations and policies. The Contractor shall provide the expertise to utilize these tools throughout the SDLC for the project, including, at a minimum:</p> <ul style="list-style-type: none"> <li>a) Database Security Monitoring and Compliance Reporting (Oracle Audit Vault or functional equivalent)</li> <li>b) Vulnerability Scan (Nessus or functional equivalent)</li> <li>c) Security Information and Event Management (Qradar or functional equivalent)</li> <li>d) Static Code Checking (Fortify or functional equivalent)</li> <li>e) Log Server (SysLog Server or functional equivalent)</li> <li>f) File Integrity Checker (Advanced Intrusion Detection Environment or functional equivalent)</li> <li>g) Virus Scan (Symantec Endpoint Protection (Windows), Clam Antivirus (Linux), or functional equivalent)</li> <li>h) Compliance and Information Security Program Management (Lockpath Keylight or functional equivalent)</li> <li>i) Identity and Access Management (Oracle Identity and Access Management or</li> </ul>

Term	Definition
	<p>functional equivalent)</p> <p>j) System Monitoring (Sitescope or functional equivalent)</p> <p>k) Application Scanning (NetSparker Server or functional equivalent)</p>
<b>Security Compliance Testing</b>	A Security Test & Evaluation (ST&E) will validate all applicable security controls defined in the CMS Policy for the Information Security Program. ST&E validates that business application or infrastructure are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the application or infrastructure. ST&E may include vulnerability scanning, penetration testing, and/or testing security standards and policy.
<b>Security Control Assessment</b>	Addresses how the evaluator shall perform active security testing of the information system to assess the implemented security controls and to identify gaps between the implemented controls and the documented controls. The evaluator shall capture, document and retain information sufficient to prove the existence or non-existence of vulnerabilities discovered through the assessment process. Any gaps identified during the documentation review, interviews or security control assessments will be reported in the findings report based on the CMS Reporting Procedure for Information Security Assessments.
<b>Smoke/Sanity Testing</b>	Smoke Tests are shallow and wide, testing all areas of the application without getting deep in focus. Sanity tests are narrow and deep regression tests, testing one or a few areas of functionality. These tests are used to determine if an environment or Release is stable enough to begin a testing cycle.
<b>Solution or System</b>	Solution describes features, functions, and characteristics of the product, system, service, or result that will meet the business and stakeholder requirements.
<b>Stakeholder Management Process</b>	The Stakeholder Management Process is used to identify the project's key stakeholders and their roles and responsibilities within the project, provide an analysis of their interests in and attitude towards the effort, and manage stakeholder participation to secure positive support for the project. The Stakeholder Management process capability identifies the impacted groups or individuals and their needed level of commitment and establishes detailed engagement plans for impacted stakeholders to ensure project success.
<b>Successful Release</b>	All designed capabilities are operational according to specification and the State accepts the Go-Live deliverable
<b>Technical Sandbox</b>	The Technical Sandbox is an isolated and restricted computer environment where developers conduct testing on untested and untrusted codes. A restricted environment is created to ensure stability and security.
<b>Test Management Tool</b>	Repository for all test documents, cases, results, statues, and how testing was done. The testing repository will include all automated and manual activities.
<b>Time-travel</b>	Ability to future-date or back-date operating system date in order to assist in testing of functionality related to time-driven events.
<b>Unit Testing</b>	Unit Testing is performed by the system developer/maintainer subsequent to or in parallel with application development to assess and correct the functionality and data of a business application's individual code modules.
<b>Usability Testing</b>	Testing technique typically performed by end users to verify the appropriate level of ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component.
<b>User Acceptance Testing</b>	Assess and accept the overall functionality and interoperability of a business application's solution in an operational mode. UAT allows end users to use the solution in a manner that most resembles actual production use. Testing is performed against the Business Product/Code based on the user's requirements, and may include Training Artifacts and User Manual. UAT may also assess the user's experience with the application to determine if users are able to accomplish their tasks and goals satisfactorily and efficiently to help identify potential problems and possible improvements (i.e., usability testing). Success in UAT will result in a sign-off by the business owner, validating that the business application meets documented requirements.
<b>Worker Portal</b>	The Worker Portal shall provide Solution access to member services workers, appeals unit workers, service center staff (TNHC intake, including intake for CHIP & the Redetermination Vendor), State office users outside of member services, including internal audit, policy, fiscal, and help desk, Department of Children's Services (Foster Care), and other Department of Health (DOH) application intake. The Worker Portal shall be accessible both

<b>Term</b>	<b>Definition</b>
	within the State of Tennessee network, and outside of the State of Tennessee network.

**Contract ATTACHMENT 8**

---

---

**PROPOSER'S LIBRARY**

Content available for the Proposer's Library located at <http://tn.gov/tenncare/article/rfq>

- 1 - A.17 EA-BOM Plan
- 2 - A.25 Project and Systems Development Lifecycle Management Plan
- 3 - A.30 Requirements Managements Plan
- 4 - A.33 Testing Management Plan
- 5 - A.34 Interface/Integration Management Plan
- 6 - A.41 Integrated Program Operations & Maintenance Planning/Deployment Plan
- 7 - A.46 Organizational Change Management and Training Plan (Extract)
- 8 - A.47 Communication Management Plan (Extract)
- 9 - A.49 Program Governance Management Plan
- 10 - State of Tennessee Call Center Volumetrics
- 11 - State of Tennessee Application Volume Report
- 12 - State of Tennessee Suggested System Components
- 13 - Cisco TelePresence Conferencing Specs
- 14 - Cisco TelePresence Touch Devices
- 15 - State of Tennessee Enrollee 7 Match and 4 Match Criteria
- 16 - State of Tennessee MMIS Interface Specifications
- 17 - MARS-E 2.0 Document Suite
- 18 - FTI and e-Authentication Documentation
- 19 - State of Tennessee Enterprise Technology Architecture
- 20 - Health Care Finance and Administration Organizational Chart
- 21 - Health Care Finance and Administration Business Operating Model Design
- 22 - Health Care Finance and Administration Roadmap Report
- 23 - CMS Critical Success Factors (EE CSF 2016-02-18)
- 24 - CMS Seven Standards and Conditions
- 25 - MITA 3.0 Documentation

26 - STS Processes and SLAs

27 - Health Care Finance and Administration Eligibility Policy

28 - Health Care Finance and Administration COTS Technology Components

29 - State of Tennessee MAGI Based Eligibility Verification Plan

30 - CMS Computer Matching Agreement

31 - Interconnected Systems Agreement Template

32 - State of Tennessee MMIS Interface List

33 - FIPS-PUB-199-final

34 - A.50 Quality Management Plan (Extract)

---

## DETAILED CURRENT STATE, FUTURE STATE, AND ROADMAP INFORMATION

### 5.7 Current State Overview

- 5.7.1 The State of Tennessee Department of Finance and Administration, Division of Health Care Finance and Administration (HCFA), hereinafter referred to as the "State" or "HCFA", operates the federal Medicaid program in Tennessee known as "TennCare" through its Bureau of TennCare (Bureau), pursuant to Waivers granted by the CMS. HCFA also operates the federal CHIP, in Tennessee known as "CoverKids" (collectively referred to herein as "CoverKids" or "CHIP"). Eligibility determination and related responsibilities for TennCare and CoverKids are handled through a combination of State staff and State contractors.
- 5.7.2 Tennessee is modernizing and streamlining the eligibility determination and appeals processes for all health coverage programs administered by the State. The current system is disjointed, resource intensive, burdened by inefficient manual interventions, and difficult for workers to navigate. Tennessee does not have a single system which determines eligibility for all Medicaid and CHIP categories. Rather, it relies on multiple entities, systems and manual processes to adjudicate applications. As a determination state, Tennessee relies on the FFM to determine MAGI-based eligibility for Medicaid and CHIP. The State adjudicates eligibility for all non-MAGI eligibility categories (e.g., services for individuals needing long term services and supports).
- 5.7.3 The lack of integration of the current information technology environment adversely affects the business processes and operations. Various bridge systems and standalone micro-systems have been developed over time due to limitations of the mainframe platform and the need to provide functionality for workers to meet statutory and regulatory requirements. The IT environment operates in silos across HCFA and is supported by numerous Contractors and technologies. This results in increased workload for staff serving applicants and members.
- 5.7.4 In December 2012, The State of Tennessee awarded a contract to provide and operate a new web based system to meet the requirements of the PPACA and determine eligibility for Medicaid and CHIP benefits. For this project, called the Tennessee Eligibility Determination System (TEDS), the Solution was intended to leverage a product which had been implemented in another state, in order to accelerate the implementation of TEDS. The project faced persistent schedule, quality, and resource challenges and was canceled prior to implementation.
- 5.7.5 HCFA is undertaking a large-scale Medicaid Modernization Program (MMP or Program) to modernize its eligibility system and programs. The MMP includes (a) information technology (IT) systems relating to TennCare and CoverKids (including the Medicaid Management Information System (MMIS)), and (b) the TennCare and CoverKids eligibility determination processes. The Eligibility Modernization Program (EMP) represents the State's highest priority in the MMP Program. Major features of the TEDS include a rules-based decision engine, enabling eligibility determinations that are fully compliant with the PPACA, CMS requirements and all applicable State and Federal regulations. The new system shall be able to interface with the Federal HUB in order to perform verifications and make real-time TennCare and CHIP eligibility determinations.

- 5.7.6 The current system is operated by the Tennessee Department of Human Services' (DHS) ACCENT. ACCENT is used, in part, to determine Medicaid eligibility. Significant customization of this system has been required to meet Tennessee's requirements. ACCENT is an integrated system that was built on legacy mainframe technologies. It supports eligibility processing for Temporary Assistance for Needy Families (TANF), the Supplemental Nutrition Assistance Program (SNAP), and Medicaid. ACCENT is unable to meet the requirements of the PPACA, both from business and technology requirements perspectives.
- 5.7.7 HCFA's approach to modernization is to:
- 5.7.7.1 Discontinue use of ACCENT for eligibility determination for Non-MAGI Medicaid programs;
  - 5.7.7.2 Transition from a "determination" State to an "assessment" State for MAGI-based eligibility; and
  - 5.7.7.3 Establish a single system to determine eligibility for all State-administered health coverage programs.
- 5.7.8 As part of HCFA's eligibility modernization efforts, the following systems will require either modification or replacement:
- 5.7.8.1 Replace existing legacy mainframe eligibility determination system (ACCENT) with regard to Medicaid eligibility;
  - 5.7.8.2 Replace legacy CHIP eligibility and enrollment processes and systems;
  - 5.7.8.3 Create eligibility related interfaces between MMIS and TEDS;
  - 5.7.8.4 Replace the Tennessee Eligibility Appeals Management System (TEAMS); and
  - 5.7.8.5 Streamline and automate applicant/member notification processes and systems.
- 5.7.9 The MMP must incorporate and comply with all applicable federal and State laws, rules, regulations, sub-regulatory guidance, executive orders, CMS TennCare Waivers, and all current, modified or future Court decrees, orders or judgments applicable to the TennCare and CHIP programs (collectively referred to herein as the Applicable State and Federal Requirements). These include, but are not limited to:
- 5.7.9.1 PPACA
  - 5.7.9.2 MARS-E
  - 5.7.9.3 IRS Pub 1075
  - 5.7.9.4 SSA Teleservice Representative
  - 5.7.9.5 Health Insurance Portability and Accountability Act (HIPAA)
  - 5.7.9.6 CMS Seven Conditions and Standards, and MITA 3.0.
- 5.7.10 Specific business and technical needs to be addressed include:
- 5.7.10.1 Multiple processes and systems that are currently used to determine eligibility for TennCare and CoverKids;

5.7.10.2 Significant manual interventions required to process health coverage program applications;

5.7.10.3 MMIS serves as a single system of record;

5.7.10.4 No single reference point for member services to access in order to provide applicants with information on pending applications;

5.7.10.5 Insufficient and incomplete data from the FFM to assist with inconsistencies/conflicts in application information and the resolution of appeals; and

5.7.10.6 Inability of residents to submit applications via a State-supported web portal.

## 5.8 Current State – Programs to be Automated

- 5.8.1 The TEDS requires the full spectrum of Medicaid programs to be included over the course of the development roadmap. In addition to the automation of eligibility rules for determination, any unique processing requirements will be represented in the process flows for these programs in the previous section.

*Table: Medicaid Program*

MEDICAID CATEGORY	PROGRAM	DESCRIPTION
Children	Age 0-19	Low income children age 0 up to 1 <sup>st</sup> birthday
		Low income children age 1 to 6 <sup>th</sup> birthday
		Low income children age 6 to 19th birthday
	Child Medically Needy	Children up to age 21. Must either have low income or have sufficient unreimbursed medical bills to spend down to requisite income limits.
	Standard Uninsured	Children under age 19 who do not have access to insurance. Category is only open to children who lose Medicaid eligibility and rollover into Standard.
	Standard Medically Eligible	Children under age 19 who do not have access to insurance and who have health conditions that make the child uninsurable. Category is only open to children who lose Medicaid eligibility and rollover into Standard.
	CoverKids	Available to children under age 19 and to the unborn children of women not eligible under another TennCare category.
DCS Custody/Adoption Assistance	Immediate eligibility is provided for children whom are currently in State of Tennessee DCS custody, or is receiving federal adoption assistance payments.	
Families	Caretaker Relative	Available to parents and caretaker relatives of dependent children under age 19.
	Transitional/Extended Medicaid	Children, pregnant women, and caretaker relatives who lose Medicaid due to an increase in income or spousal support.
Women	Pregnant	Low income pregnant women. NOTE: Newborns born to Medicaid –eligible women are deemed eligible for one year.
	Breast or Cervical Cancer	Women under 65 who are not eligible for any other category of Medicaid and have been diagnosed as the result of a screening at a Centers for Disease Control and Prevention site.
	Pregnant Medically Needy	Pregnant women. Must either have low income or have sufficient unreimbursed medical bills to spend down to requisite income limits.
Aged, Blind, &	SSI (Supplemental	Active: Low income aged, blind, or disabled recipients of federal SSI

MEDICAID CATEGORY	PROGRAM	DESCRIPTION
<b>Disabled</b>	Security Income)	cash payments as determined by SSA
	Long Term Services and Supports	Low income individuals who require care in a nursing facility or intermediate care facility for individuals with intellectual disabilities or who receive Home and Community-Based Services in their home.
	SSI-Related (Pickle/Pass Along, Disabled Adult Child, Widow/Widower)	Pickle/Pass Along: Lost SSI since 1977 due to OASDI cost-of-living increase. DAC: Lost SSI since 1987 due to receipt/increase of DAC benefits. Widow/Widower: Lost SSI due to receipt of OASDI from deceased spouse.
<b>Adult Foster Care</b>	Former Foster Care Up to Age 26	Individuals under age 26 who aged out of foster care in Tennessee and who received TennCare Medicaid at that time.
<b>Emergency Medical Services</b>	Emergency Medical Services	Individuals who would qualify in one other category but does not have an appropriate immigration status
<b>Medicare Cost Sharing</b>	Qualified Medicare Beneficiary	TennCare pays Medicare premiums, deductibles and coinsurance for those eligible for Medicare.
	Specified Low Income Medicare Beneficiaries	TennCare pays Medicare Part B premiums only.
	QI 1	Qualified Individuals TennCare pays Medicare Part B premiums only.
	Qualified Disabled Working Individual	TennCare pays Medicare Part A buy-in for non-aged individuals who lost SSI disability benefits and premium free Part A.
<b>Presumptive</b>	Hospital Presumptive	Temporary coverage for application submitted at participating hospitals for: children (ages 0-18) parents caretaker relatives pregnant women former foster care children between the ages of 18-26
	Pregnancy Presumptive	Temporary coverage for pregnant women.
	Presumptive Breast and Cervical Cancer (BCC)	Temporary coverage for those individuals eligible for BCC category.

5.8.2 The following are estimates of enrollees for existing Medicaid categories:

5.8.2.1 SSI – 231,468

5.8.2.2 Institutional/HCBS/SSI-Related – 32,564

5.8.2.3 SSI Related – 19,125

5.8.2.4 DCS/Adoption Assistance – 27,946

5.8.2.5 Pregnant Women, Children, Caretaker relatives – 1,028,244

5.8.2.6 Newborns – 95,314

5.8.2.7 Presumptive Pregnant Women – 21,746

5.8.2.8 Breast and Cervical Cancer – 2,957

5.8.2.9 Medically Needy – 28,459

## 5.8.2.10 Standard Children – 18,662

**5.9 Future State – Business Overview**

- 5.9.1 The State is planning for a client service model that is customer-centric, efficient and effective. This service model is to provide a consumer friendly end-user experience. Excluding applications for Supplemental Security Income (SSI) benefits who will continue to file applications directly through the Social Security Administration (SSA), TennCare and CoverKids applicants and members will need to be able to both file applications for services, submit requested verifications or additional information, as well as report changes using multiple electronic channels and processes. Once core capabilities are operational, the State has also included in its Roadmap the establishment of a mobile application that would allow applicants and members to access the eligibility process and their electronic case record through a mobile device.
- 5.9.2 When TEDS is fully deployed, most required materials and verification documents will be scanned and stored electronically within the applicant's or member's electronic case record. Whenever possible, verification of required information will be captured electronically through a web-based service and updated automatically in the case record. Workers or automated processes will review applications and send questions or request additional documentation electronically or through print media to communicate with applicants and members.
- 5.9.3 In order for HCFA to achieve the following strategic business objectives, the TEDS will:
- 5.9.3.1 Provide a “no wrong door” to all health coverage programs administered by the State;
  - 5.9.3.2 Provide workers with access to up-to-date member records across all Medicaid health coverage programs;
  - 5.9.3.3 Automate eligibility determination to provide real-time or near real-time responses to applicants; and rely on human intervention only when requested by the applicant/member or required by program policy;
  - 5.9.3.4 Align eligibility processes to meet the needs and preferences of applicants, members, stakeholders, business partners and HCFA workers and contractors;
  - 5.9.3.5 Improve the ability to collect complete, relevant, timely and accurate data to be used for eligibility, including eligibility appeals;
  - 5.9.3.6 Leverage Service Oriented Architecture (SOA) principles to develop an extensible architecture that will comply with CMS' Medicaid Information Technology Architecture (MITA), CMS' Seven Conditions and Standards, and national standards for security, privacy, interoperability and information sharing;
  - 5.9.3.7 Manage eligibility criteria in a transparent and collaborative manner that allows for efficient and appropriate updates;
  - 5.9.3.8 Accommodate business, regulatory and technical changes to the eligibility system in a timely, non-disruptive fashion
  - 5.9.3.9 Maximize use of automation where possible.

## 5.10 Future State – Guiding Principles

- 5.10.1 Tennessee has identified five (5) guiding principles to prioritize decisions for the future state of eligibility operations:
- 5.10.1.1 Consistent delivery of member services and increased member self-service
  - 5.10.1.2 Expand and improve eligibility intake channels via contact center and online portal to increase applicant and member satisfaction;
  - 5.10.1.3 Provide citizens with the ability to apply for services and benefits at a time and place convenient for them through an accessible web portal, utilizing agency and contract staff only when necessary;
  - 5.10.1.4 Provide real-time or near real-time eligibility determinations, without agency worker intervention, and improve the accuracy of eligibility determinations;
  - 5.10.1.5 Reduce unnecessary manual intervention by HCFA workers by providing self-service functionality for clients to access eligibility applications, submit documentation and update personal information;
  - 5.10.1.6 Provide information to applicants and members in a manner of their choosing (e.g., paper, electronic);
  - 5.10.1.7 Utilize a single contact center for all eligibility-related services; and
  - 5.10.1.8 Provide HCFA member services (e.g., contact center staff) with on-line access to information needed to respond to member inquiries.
- 5.10.2 Optimized business operations using reliable systems
- 5.10.2.1 Provide a high level of automation and systems adaptability throughout the eligibility process;
  - 5.10.2.2 Minimize complexity of user interfaces to perform systems functions;
  - 5.10.2.3 Implement a content management system (including document management) in compliance with State and federal regulations and statutes;
  - 5.10.2.4 Reduce the cost of future technology enhancements by implementing modular components;
  - 5.10.2.5 Define and institutionalize business processes, operational changes and eligibility rules throughout the agency;
  - 5.10.2.6 Establish an automated system to generate notices and letters to applicants, members, stakeholders and business partners; and
  - 5.10.2.7 Consolidate data currently housed in separate systems into a single system, reducing the need for HCFA staff and Contractors to access multiple systems/databases.
- 5.10.3 Enhanced program self-sufficiency
- 5.10.3.1 Transfer responsibility for MAGI-based eligibility determination from the FFM to HCFA;

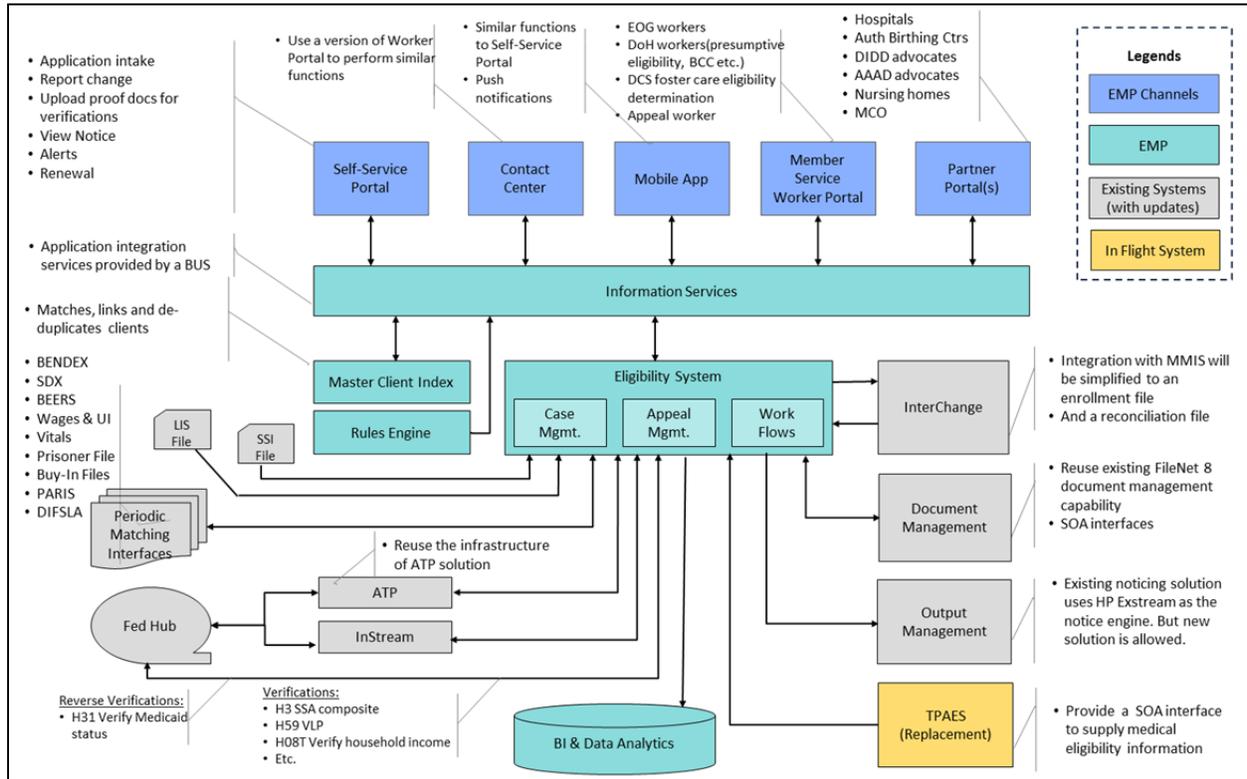
- 5.10.3.2 Improve sustainability of systems and operations;
  - 5.10.3.3 Reduce the need for contracted staff to aid applicants and members;
  - 5.10.3.4 Lower average transaction costs through automation of eligibility determination;
  - 5.10.3.5 Facilitate more accurate and timely adjudication of eligibility appeals by consolidating information in one system and providing appeals staff with access to a centralized data source and single system of record; and
  - 5.10.3.6 Adapt staffing levels to reflect new model/systems and volume of caseload.
- 5.10.4 Organizational adaptability
- 5.10.4.1 Implement and integrate automated rules engines to enable updating of rules with less development costs when regulatory changes impact eligibility standards;
  - 5.10.4.2 Develop a system that has the flexibility to accommodate the expansion or contraction of current programs, or the establishment of new programs; and
  - 5.10.4.3 Better assess current performance and accurately project future business needs.
- 5.10.5 Improved data quality and data integrity
- 5.10.5.1 Minimize data discrepancies and improve data integrity associated with transmission of applicant eligibility determinations from FFM to HCFA;
  - 5.10.5.2 Establish governance structure to better manage data and information, including ownership and accountability;
  - 5.10.5.3 Track applications received, by pending, approved, denied and abandoned;
  - 5.10.5.4 Report performance metrics without the need for manual intervention;
  - 5.10.5.5 Audit and track member encounters;
  - 5.10.5.6 Prevent duplicate eligibility determinations by matching new and in-process applications and current Medicaid/CHIP enrollment; and
  - 5.10.5.7 Enable recognition of superseded “change of circumstance” applications to eliminate casework on previously filed applications.

## **5.11 Future State – Technical Overview**

- 5.11.1 A modular, SOA based future state architecture will be used for TEDS. The Conceptual Architecture builds a foundation of a large enterprise eligibility system and uses products from major enterprise software vendors. It supports the functional and technical requirements of a modern eligibility system and has the flexibility to support HCFA’s short and longer-term goals. The core architecture is designed such that components can be changed, added, or removed to meet HCFA’s current and future requirements.
- 5.11.2 In addition to the overarching guiding principles noted earlier, the Future State Conceptual Architecture observes the following IT principles that align with the State’s IT strategy:
  - 5.11.2.1 MITA aligned and meets CMS’s Seven Conditions and Standards.

- 5.11.2.2 Employs a layered and modularized approach to implementing system architecture. This approach cleanly separates the system's presentation layer, shared services layer and the underlying commercial off-the-shelf (COTS) products. This allows HCFA to maximize interoperability with other State systems and reduce the eligibility system infrastructure maintenance costs.
  - 5.11.2.3 Technology agnostic to allow Systems Integrators to propose mature solutions without unnecessary constraints or limitations.
  - 5.11.2.4 Leverages enterprise architecture methodology and avoids developing new systems in silos, leverages existing and ongoing HCFA investments on sharable capabilities, such as Master Person Index (MPI), enterprise service bus (ESB), identity and access management, and electronic content management (ECM).
- 5.11.3 The Conceptual Architecture for the TEDS follows the widely accepted industry standard for maintainability by separating every function into implementation layers:
- 5.11.3.1 Presentation layer – a user interface view (no storage of data)
  - 5.11.3.2 Services layer – where calculations are performed
  - 5.11.3.3 Data storage layer – where data is stored
- 5.11.4 The overall architecture, as shown in the Figure on the following page, is composed of five major features: (1) User Interfaces/Points of Access, (2) Platform, (3) Eligibility System Major Feature Groups, (4) Data Exchange with External Stakeholders, and (5) Reporting and Analysis Tools.
- 5.11.5 Each major system is depicted as a 'box'. The data flows between systems are identified, as well as the batch files used to exchange data in a recognized, standard format with the SSA, FFM and other external partners.

Figure: Future State Architecture



### 5.12 Future State – Impacted Systems

5.12.1 The new system requested will have a significant impact on the current set of systems, completely replacing some, replacing some of the existing functionality of others, and having to connect with some that remain.

Table: Impacted Systems

Application Name	Short Description
<b>Tennessee Eligibility Appeals Management System</b>	TEAMS is the name for the Tennessee Eligibility Appeals Management System. Used to track Eligibility appeals from initiation to resolution.
<b>Automated Client Certification and Eligibility Network for Tennessee</b>	ACCENT is a mainframe-based system which supports eligibility and case management functionalities for SNAP, TANF, and Medicaid. ACCENT doesn't support MAGI determination. Currently the State relies on Federally Facilitated Marketplace (FFM) for MAGI determination.
<b>EOG Core, Special, and Waiver Database (DB)</b>	An Access database that is used to track the Non-MAGI applications received from the FFM, TNHC, and SSA
<b>MAGI DB</b>	An Access database that is used to account for applications received and track eligibility related activities for the MAGI applications with inconsistencies received from the FFM.
<b>CMS Lookup DB</b>	A searchable Access database used by Resolution Specialists and others in Appeals to search for an application in the most recent CMS Data Flat File. This DB also matches the most recent CMS Data Flat File with the newest SNAP extract from DHS and contains H15 records
<b>CMS Historical DB</b>	An Access database linked to 11 other databases that contain all of the CMS Data Flat Files received since 12/20/2013. Used for a weekly APDA CIR match
<b>Account Transfer Process</b>	Given delays in the Eligibility System deployment schedule, HCFA executed an eligibility determination contingency plan to receive MAGI Applicant Eligibility Determinations and

Application Name	Short Description
	Non-MAGI Applications (Account Transfers) from the FFM and continued to use ACCENT to process un-adjudicated applications.

### 5.13 Future State – Anticipated User Counts

5.13.1 In order to plan for performance and breadth of use for TEDS systems, the following numbers of anticipated users has been provided:

#### 5.13.1.1 Worker Portal

*Table: Worker Portal*

USER GROUP TYPE	TYPE OF USE	HEADCOUNT	FTES
Member Services Workers	Worker Portal	500	400
Appeals Unit Workers	Worker Portal	195	195
Service Center - TNHC Intake - including intake for CHIP & the Redetermination Vendor	Worker Portal	500	500
State Office users outside of Member Services, including Internal Audit, Policy, Fiscal, and Help Desk	Worker Portal	130	13
Department of Human Services (DHS) Workload that will transition to Member Services with new TEDS	Worker Portal	18	18
Department of Children's Services (Foster Care)	Worker Portal	42	42
Other Department of Health (DOH) Application Intake for Presumptive BCC	Worker Portal	220	220
<b>SUBTOTAL OF WORKER PORTAL</b>		1605	1388

#### 5.13.1.2 Partner Portal

*Table: Partner Portal*

USER GROUP TYPE	TYPE OF USE	HEADCOUNT	FTES
Current TennCare Pre-Admission Evaluation System Users	Partner Portal	35	35
Nursing Homes	Partner Portal	1609	1609
Hospitals	Partner Portal	421	421
<b>SUBTOTAL OF PARTNER PORTAL</b>		2065	2065

#### 5.13.1.3 Member Portal

*Table: Member Portal*

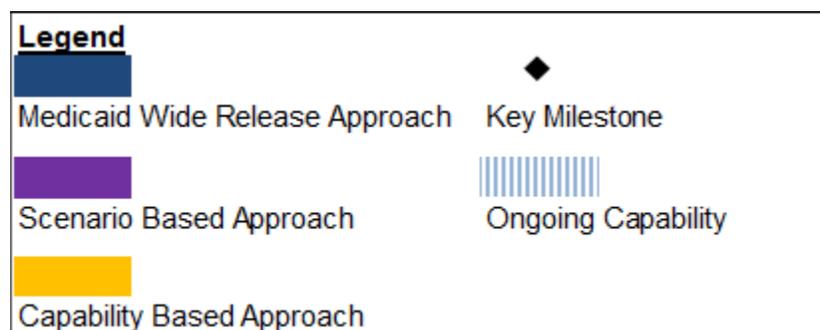
USER GROUP TYPE	TYPE OF USE	HEADCOUNT	FTES
Member Portal	Member Portal	1.5 million	N/A

### 5.14 Project Phasing

5.14.1 The Project roadmap consists of three phases and four technology-related releases. The State plans that the Contractor will initiate work in October 2016 and run through September 2020. The timeframes are estimates based on similar initiatives in other states. There are a variety of factors, however, that can impact the timelines, including the length of procurement cycles, federal approvals, and changes to federal and State statutes and regulations. The three phases are:

- 5.14.1.1 **Initial Targets (Release 1)** – Projects and initiatives that are capable of being completed within 12 to 18 months. This category of projects builds upon capabilities in order to provide the first wave of initiatives to pave the path for the future. Projects in this category include enterprise infrastructure and security, establishing a worker portal, electronic content management, and the ability to perform MAGI-based eligibility determinations. These projects form a platform that support eligibility program evolution and provide enhanced capabilities for the long term.
- 5.14.1.2 **Modernization (Releases 2&3)** – Projects in this category shall be completed within three years. The modernization starts with the addition of other Medicaid eligibility categories and builds upon the business and IT capabilities to modernize self-service channels. During this phase, certain business functions will initially have limited automation in order to meet the three-year time frame. Additionally, there may arise a need to de-prioritize certain automation capabilities in order to stay within the Roadmap schedule. These functions will be automated during the subsequent phase.
- 5.14.1.3 **Transition (Release 4)** – Projects and activities in this category relate to enhanced automation and expanded functionality of the modernized system components. Enhancements in this category include business intelligence and data analytics functionality, development of a mobile application, and enhancements to the Contact Center. Completion of these projects shall occur within four years.
- 5.14.2 The sections below summarize each of the projects (by Project Group) for inclusion within TEDS. They are broken down by Roadmap phase (Quick Wins, Modernization, and Transition) and release schedule. The Roadmap phases and release schedule are depicted by their relative time to implementation on the Gantt charts below.
- 5.14.3 In addition, the projects are divided across four primary project groupings: Enabling Projects, External Facing Projects, Worker Facing Projects, and Back Office Projects. This has been done to group those projects that have more significant dependencies so that the constraints can be readily identified and effectively managed.
- 5.14.4 The Legend for Roadmaps provides a reference for understanding the use of the colors, symbols, and patterns of the charts within this section. Solid color bars are intended to represent design and development phases. Milestones indicate a 'go-live' of the capability, with transition to maintenance phase shown as a pattern of vertical bars.

*Figure: Legend for Roadmaps*



- 5.14.4.1 Scenario-based - which implements projects focused on delivering end-to-end value for a target eligibility program type,
- 5.14.4.2 Capability-based - which implements a single functional improvement across all programs

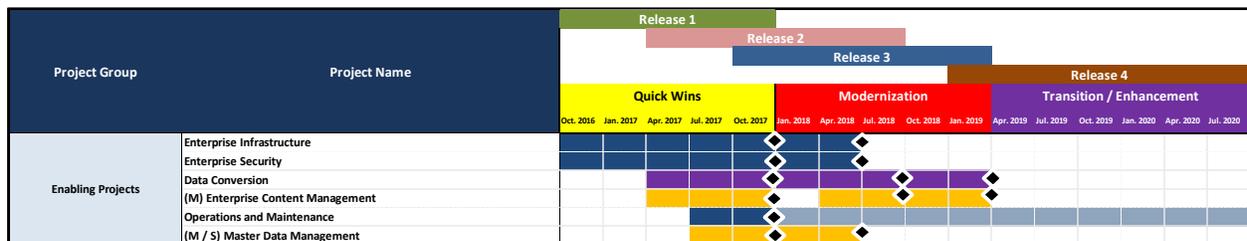
5.14.4.3 Medicaid-wide - which implements multiple functionalities simultaneously across the entire system.

5.14.5 This summary is not meant to provide an exhaustive description of each project. Instead, the brief summaries and Gantt charts below provide an overview and a sense of the scale, breadth, and timing of the initiatives to be undertaken. Each major project group is summarized as follows:

**5.15 Enabling Projects**

5.15.1 Enabling projects provide the foundation upon which modernization will occur. They are building blocks that are necessary to build a modern, modularized, and component-based system that more easily integrates with other agency technologies.

*Figure: Enabling Projects*



**5.16 External Facing Projects**

5.16.1 One of the key guiding principles the State has established is to increase the efficiency of case management processes, which can be facilitated by establishing more modern member delivery channels. As a result, external facing projects are aimed at establishing new or enhancing existing member delivery channels.

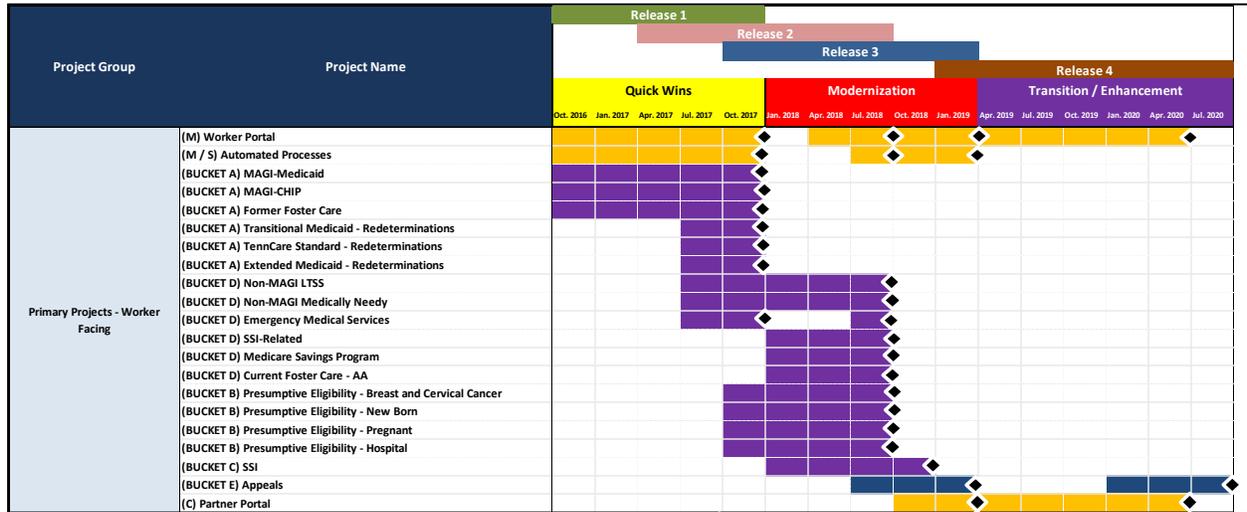
*Figure: External Facing Projects*



**5.17 Worker Facing Projects**

5.17.1 Worker Facing Projects address the needs of internal case management and actual determination. These are primarily focused on enhancing or implementing automation capabilities to improve the efficiency and effectiveness of case management processes, reduce process variance, and minimize the dependence on specialized case workers. Worker facing projects form the bulk of the implementation Roadmap. The Worker Portal shall have the ability to be accessed both within the State of Tennessee network, and outside of the State of Tennessee network.

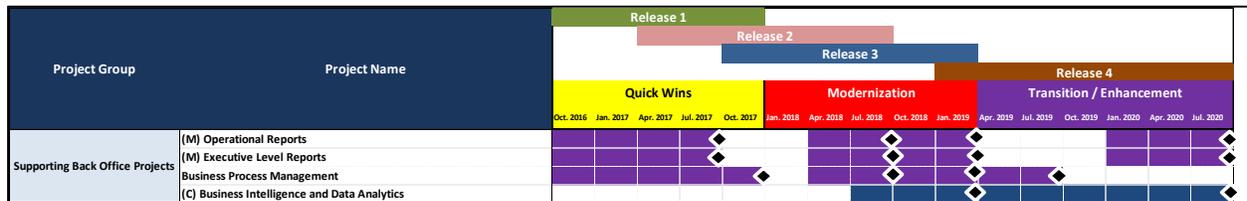
Figure: Worker Facing Projects



5.18 Back Office Projects

5.18.1 Back Office Projects are designed to support streamlined and consolidated administrative processes. These automation efforts are primarily meant to reduce the workload on case worker staff while improving task process cycle times and reducing the overall transaction cost.

Figure: Back Office Projects

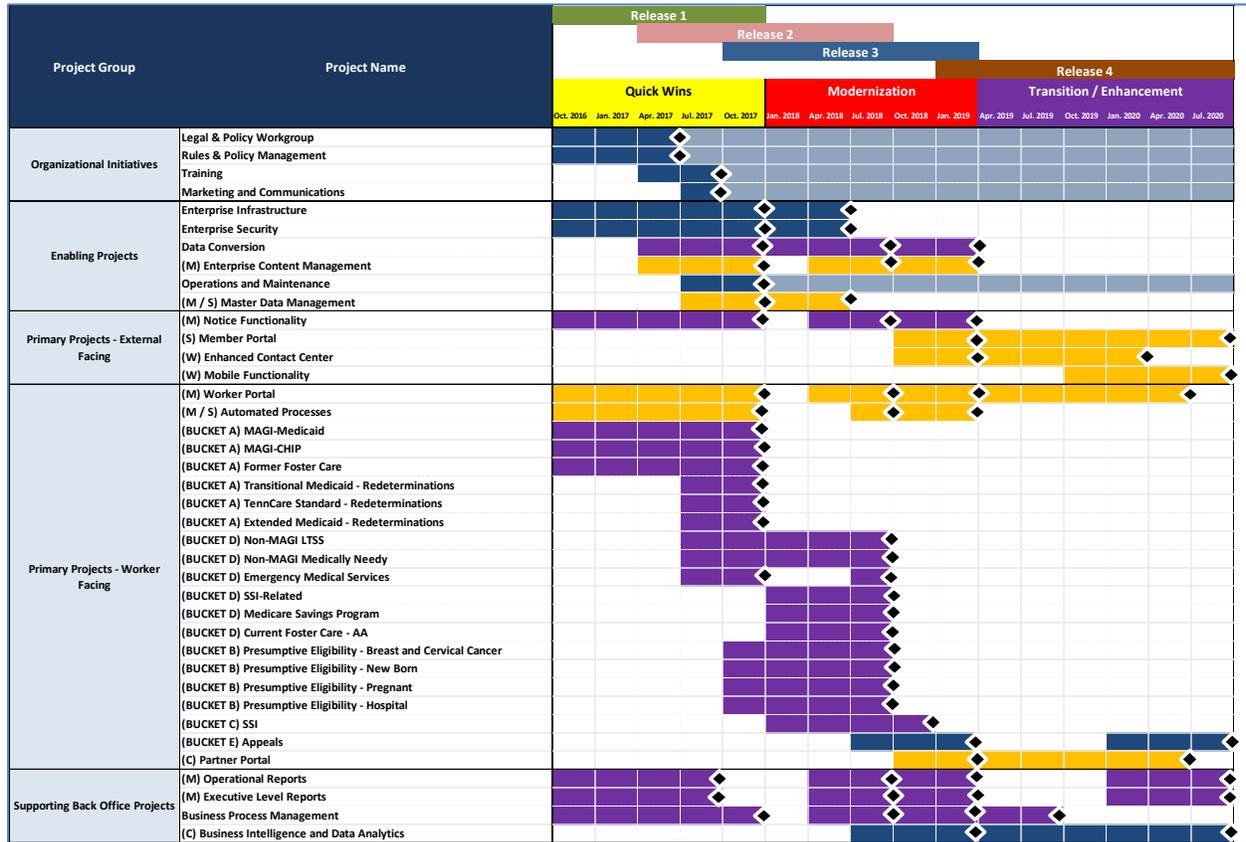


5.18.2 The State plans to take a phased approach to the modernization of its eligibility and appeals systems. The proposed schedule prioritizes the implementation of systems for eligibility categories that represent the greatest volume of lives (e.g., MAGI-based), while also improving administrative processes that will allow the State to streamline and enhance its eligibility and appeals systems.

5.18.3 As depicted in the roadmap below, the proposed schedule plans for Release 1 to be deployed and operational by December 2017, approximately 15 months after the onboarding of the Systems Integrator. This release will include functionality to determine MAGI-based eligibility for Medicaid and CHIP, among other eligibility categories, thereby enabling Tennessee to transition from a “Determination” State to an “Assessment” State. Release 2, which will be operational approximately 12 months after the deployment of the first release (i.e., January 2019), will include all Medicaid eligibility categories and will complete the transition from the interim contingency eligibility process that is currently in place to the new TEDS. Release 3 is slated to be operational in September 2019, while the final release of enhancements and additional functionality is slated to be deployed in September 2020.

5.18.4 This iterative, phased approach provides Tennessee with the best opportunity to achieve success in modernizing its eligibility system, while addressing its most pressing needs as soon as practical. For example, the State has employed a variety of legacy systems, interim solutions, manual work, outsourcing and home-grown micro-systems to meet the demand of the PPACA. In addition to replacing these systems, the State will take this opportunity to include security in a streamlined eligibility system to meet the compliance requirements of Federal and State regulation and policies.

Figure: Phased Approach



### 5.19 Business Process Flows

5.19.1 The attached business process flows represent the activities and sequencing that the new eligibility system will support.

5.19.2 Each process flow shows the level of automation that the system is expected to provide to perform each activity

5.19.2.1 Automated – Process flows/activities that will be fully automated by the Solution. In addition, any related sub-process flows and/or activities are also fully automated by the Solution.

5.19.2.2 Partially Automated – Process flows/activities that contain a combination of automated and manual sub-process flows and/or activities.

5.19.2.3 Manual – Process flows/activities that will not be automated by the Solution.

#### 5.19.2.4 External to the System – Process flows/activities that occur outside of the Solution

Figure: Level 0: Eligibility Operations

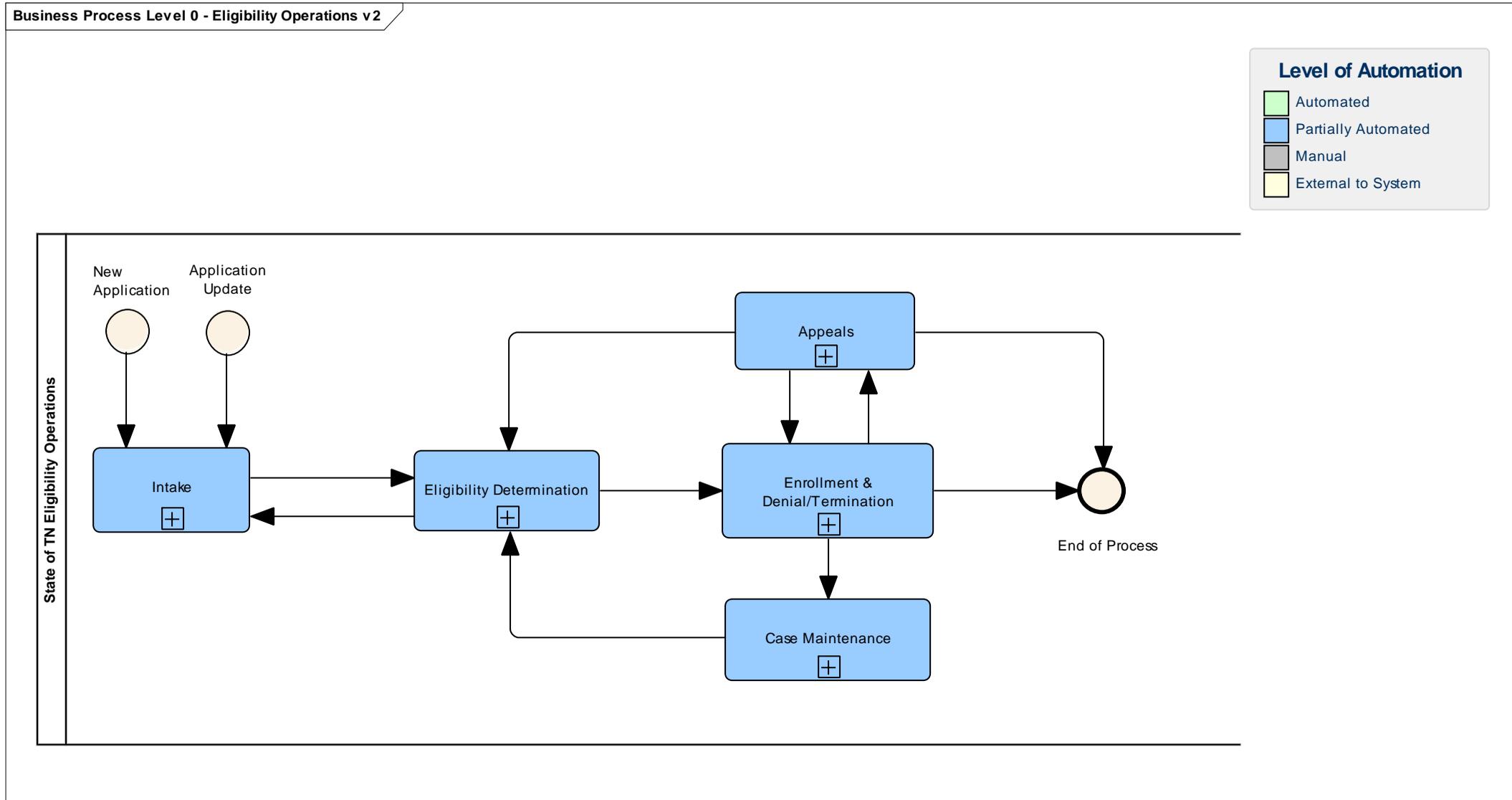


Figure: Level 1: Intake

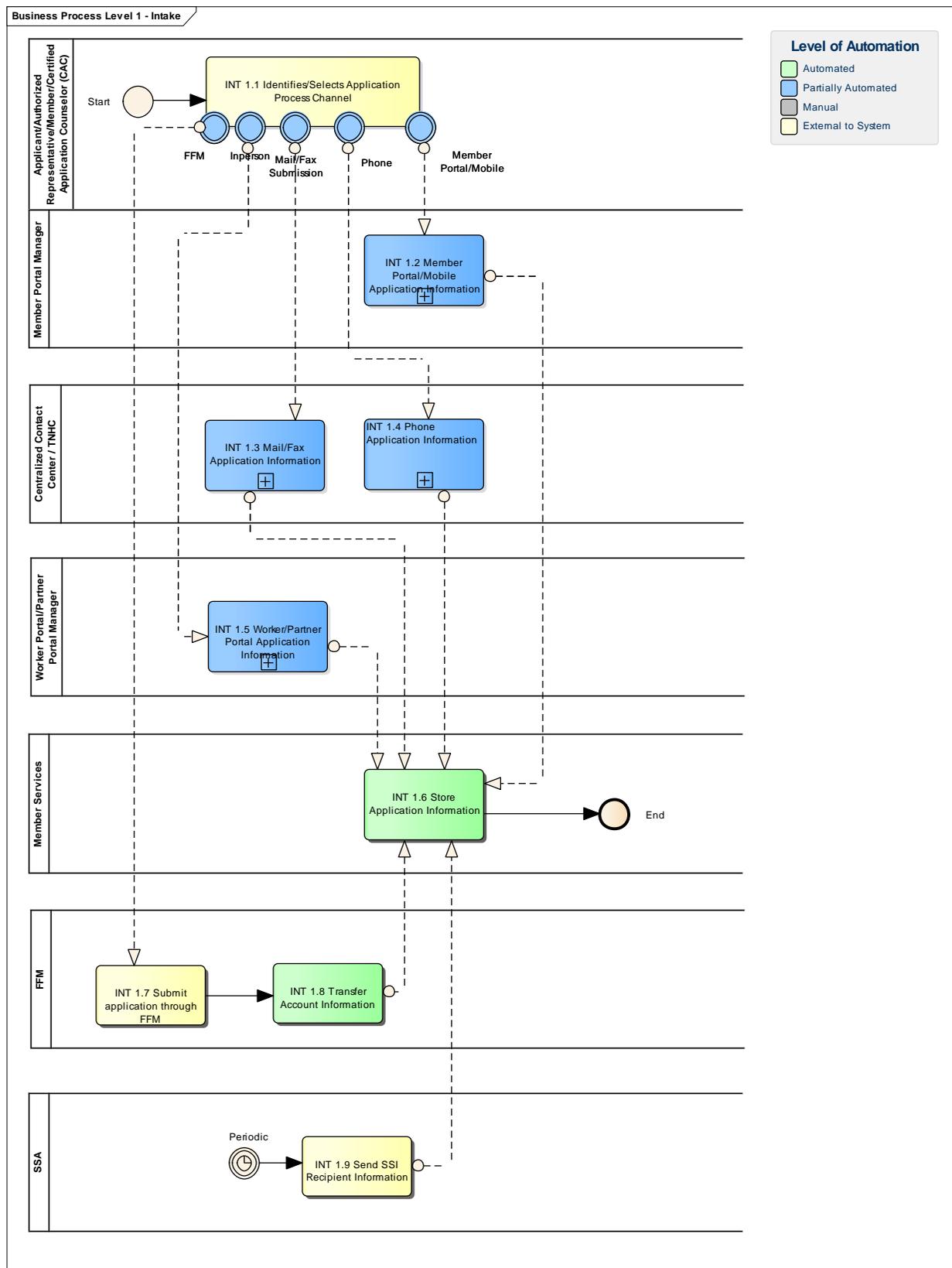


Figure: Level 2: INT 1.2 Member Portal/Mobile Application Information

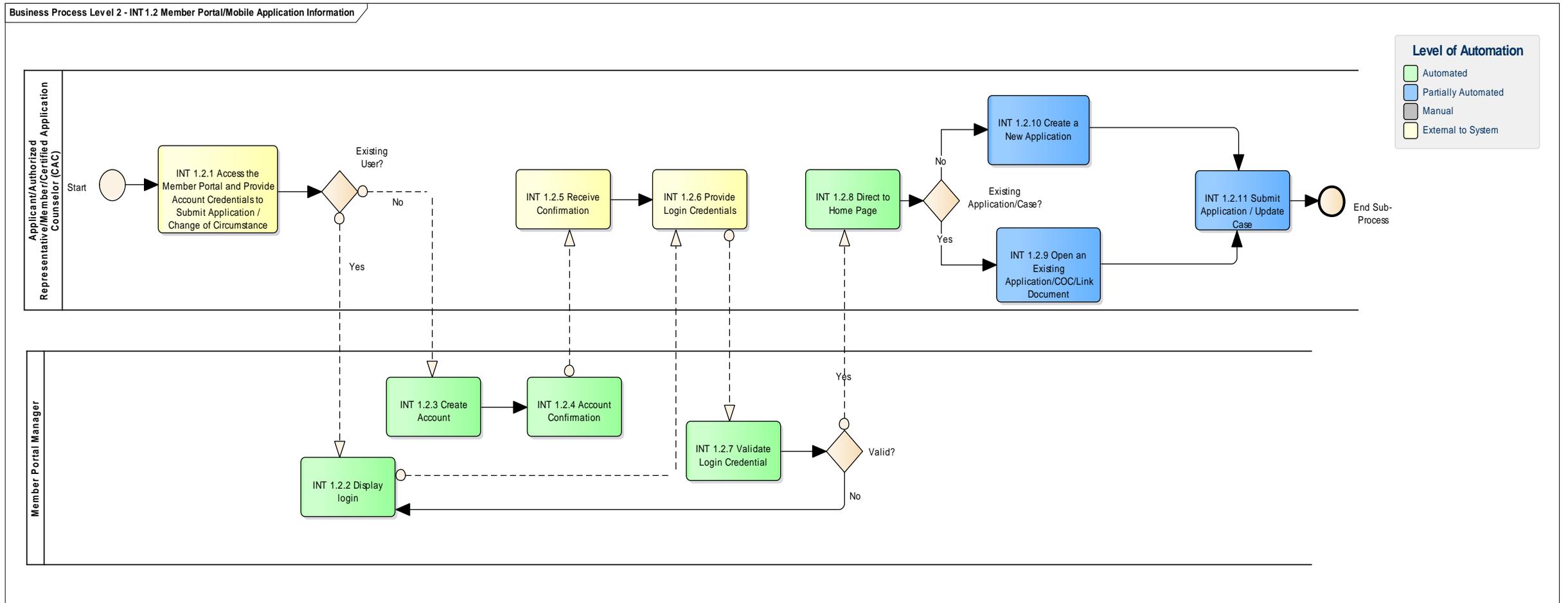


Figure: Level 2: INT 1.3 Mail/Fax Application Information

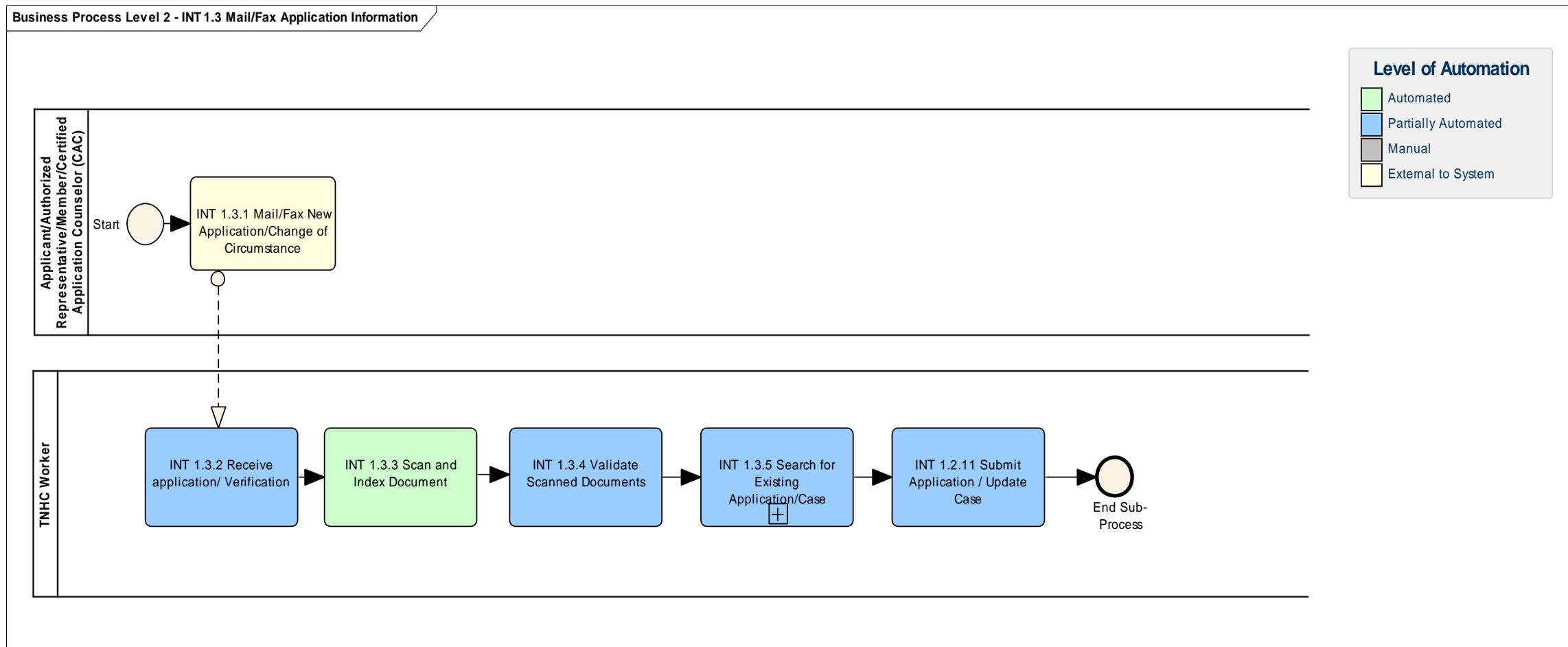


Figure: Level 3: INT 1.3.5 Search for Existing Application/Case

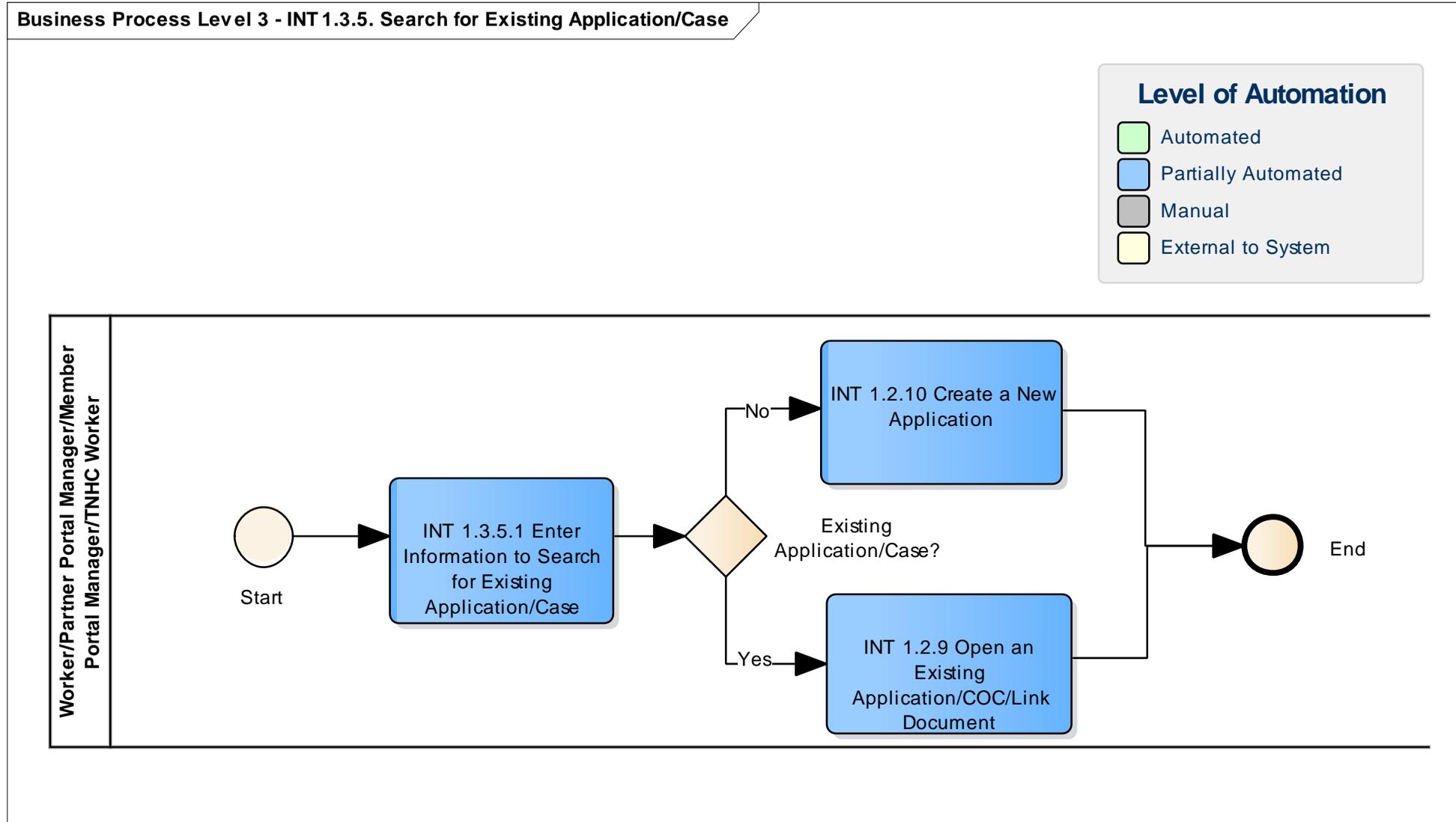


Figure: Level 2: INT 1.4 Phone Application Information

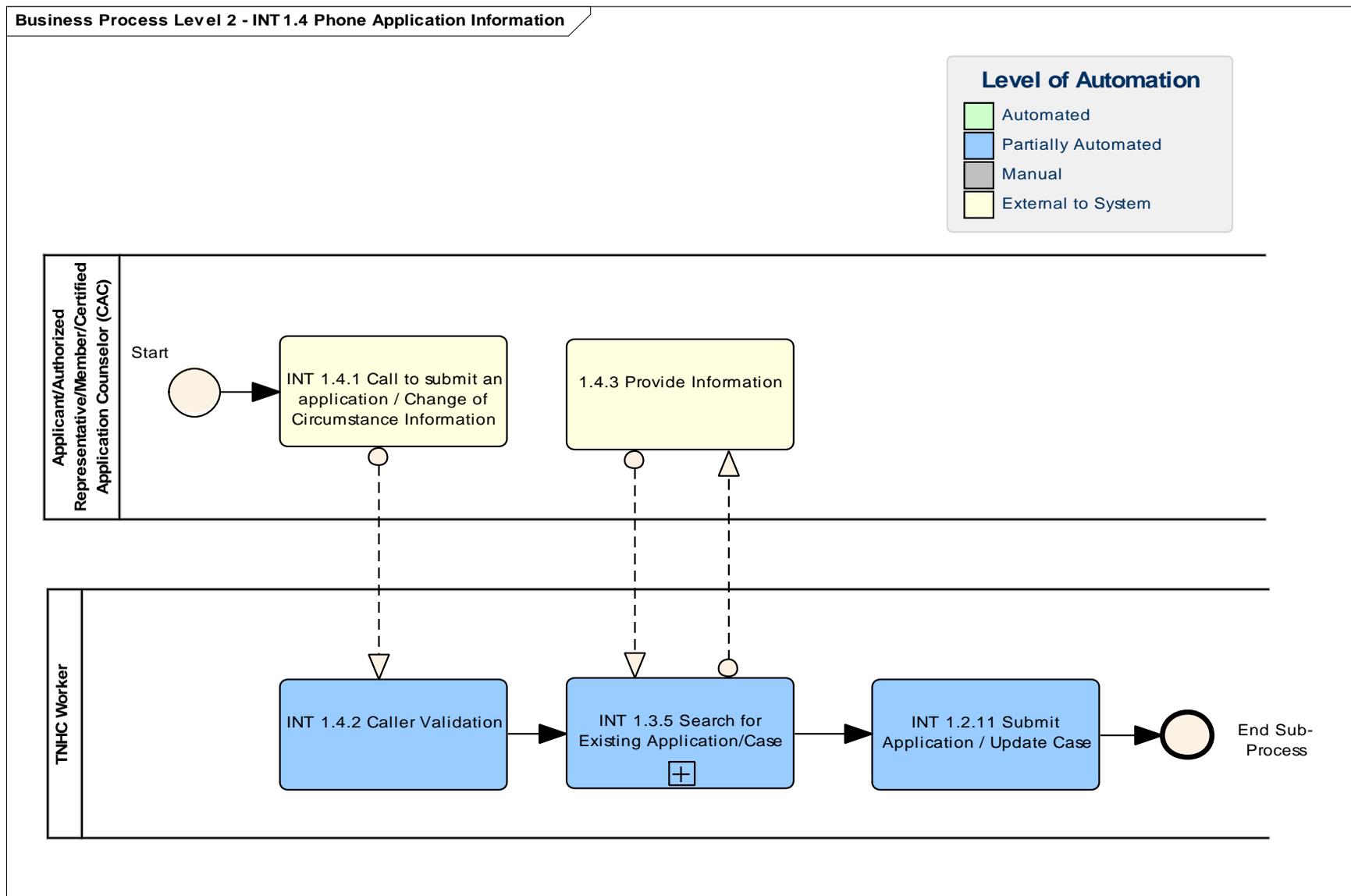


Figure: Level 2: INT 1.5 Worker/Partner Portal Application Information

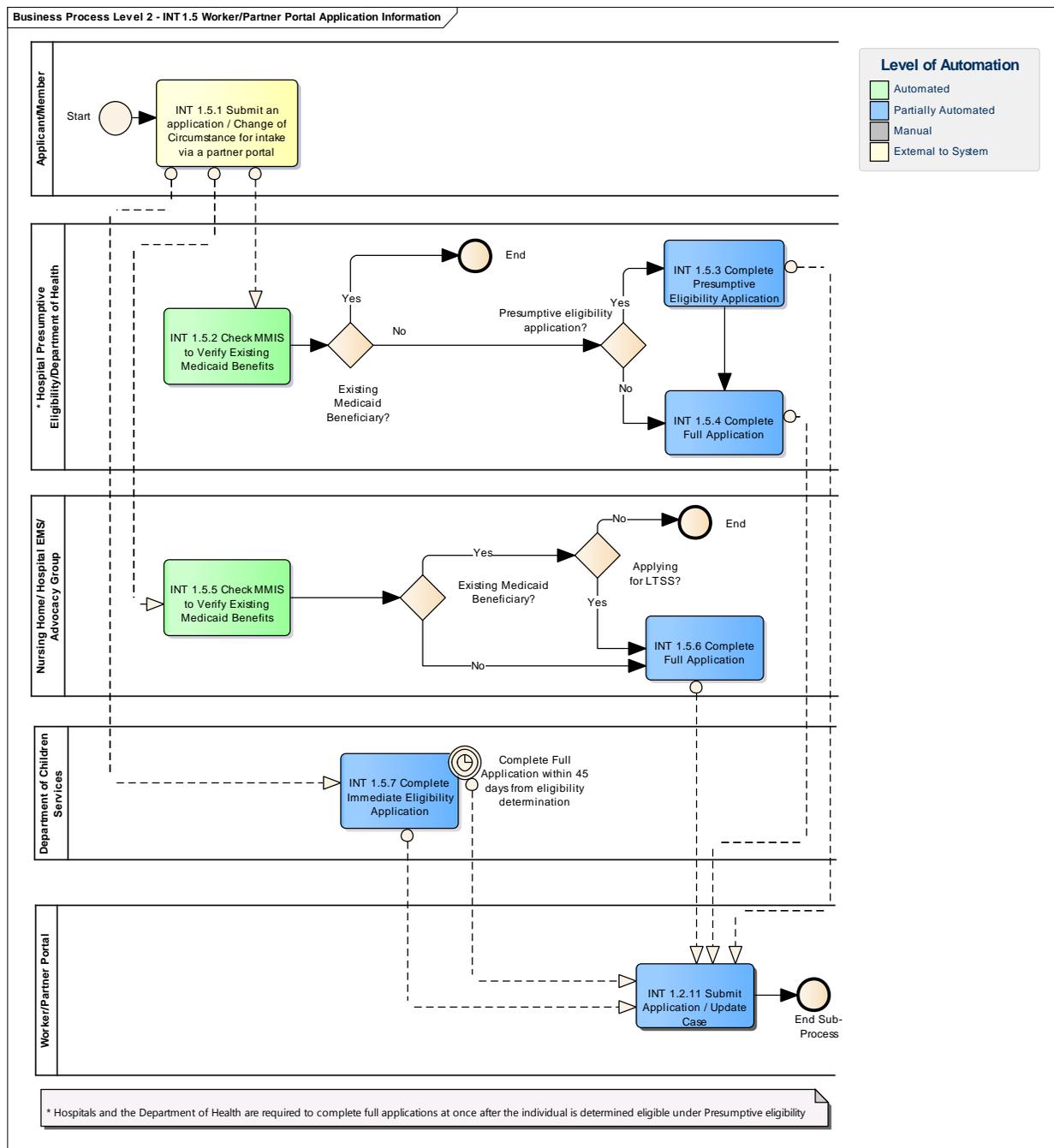


Figure: Level 1: Eligibility Determination

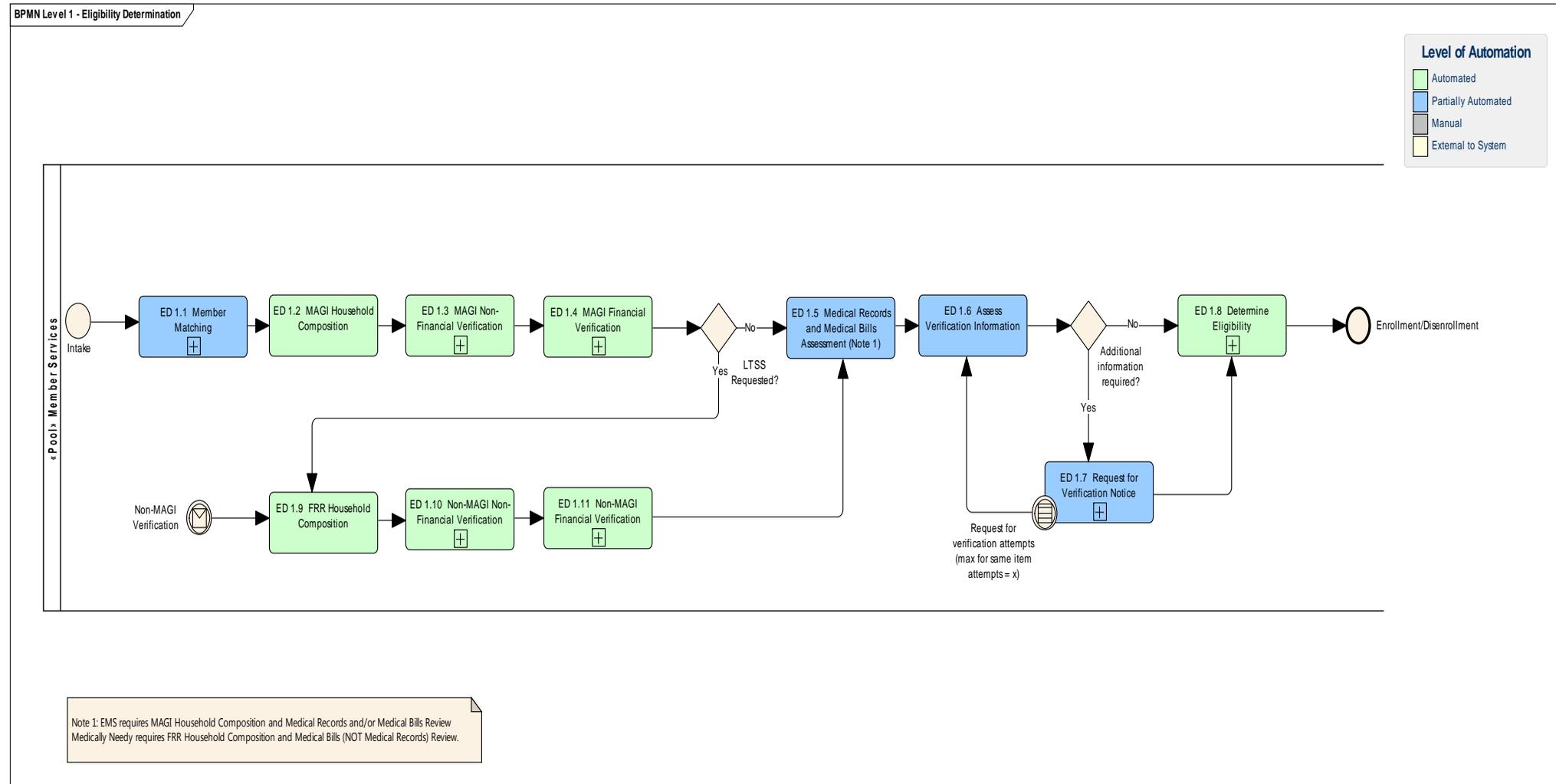


Figure: Level 2: ED 1.1 Member Matching

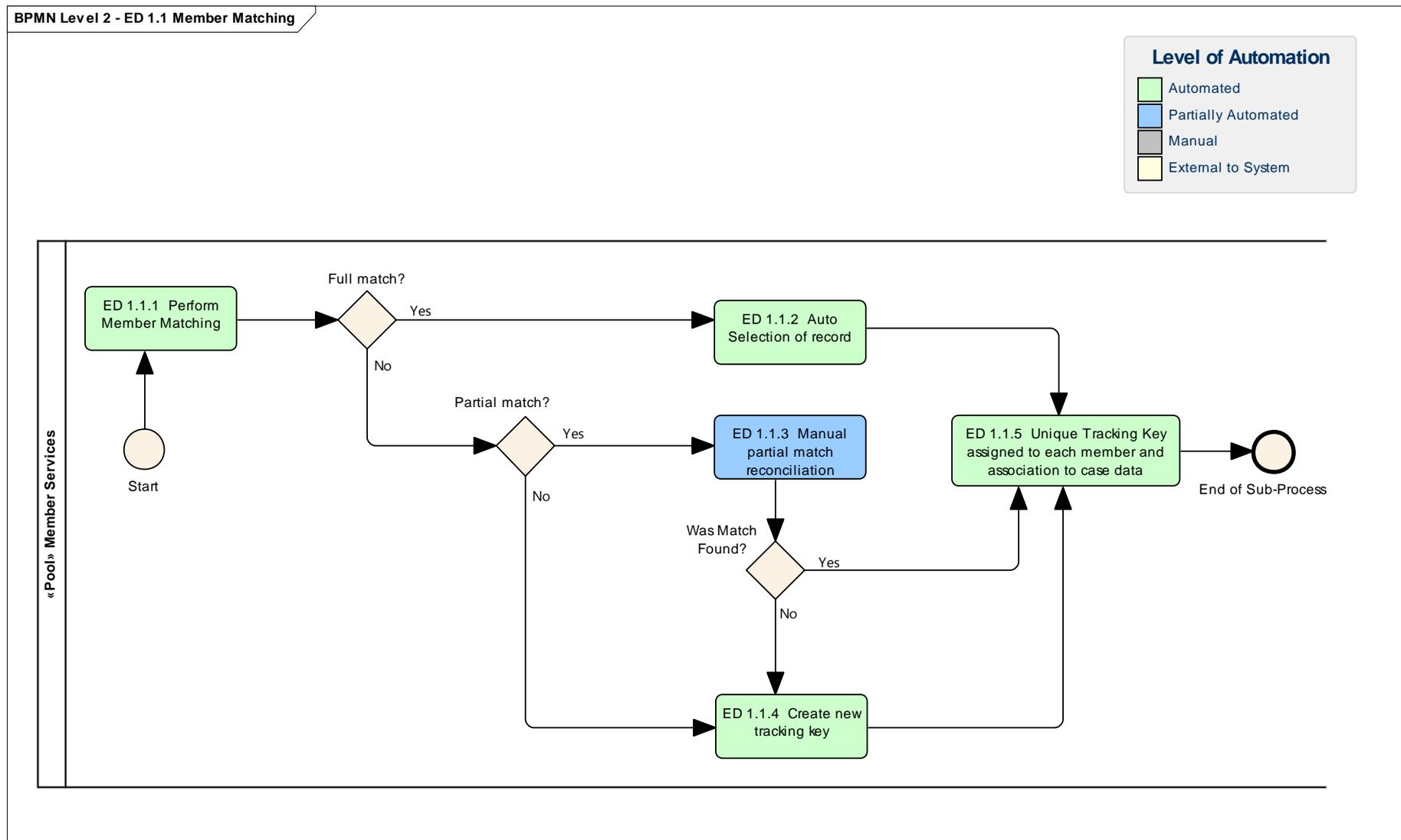


Figure: Level 2: ED 1.3 MAGI Non-Financial Verification

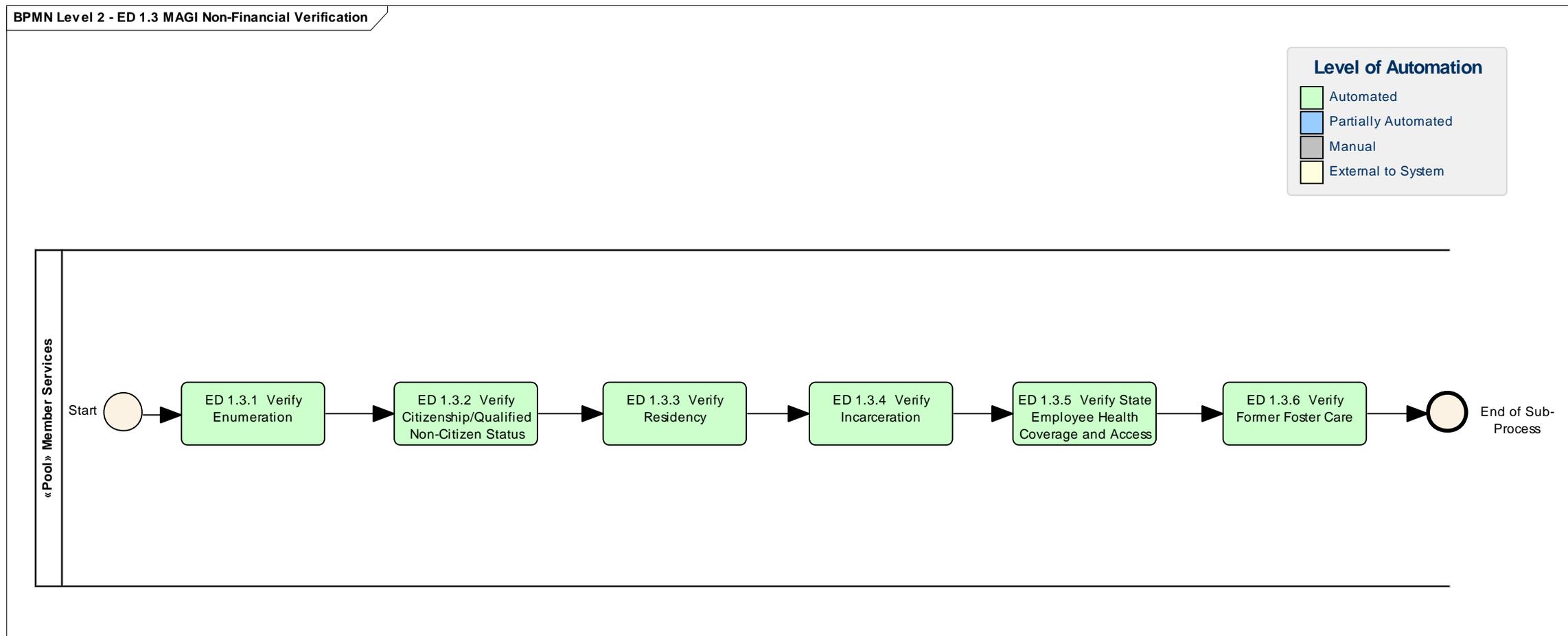


Figure: Level 2: ED 1.4 MAGI Financial Verification

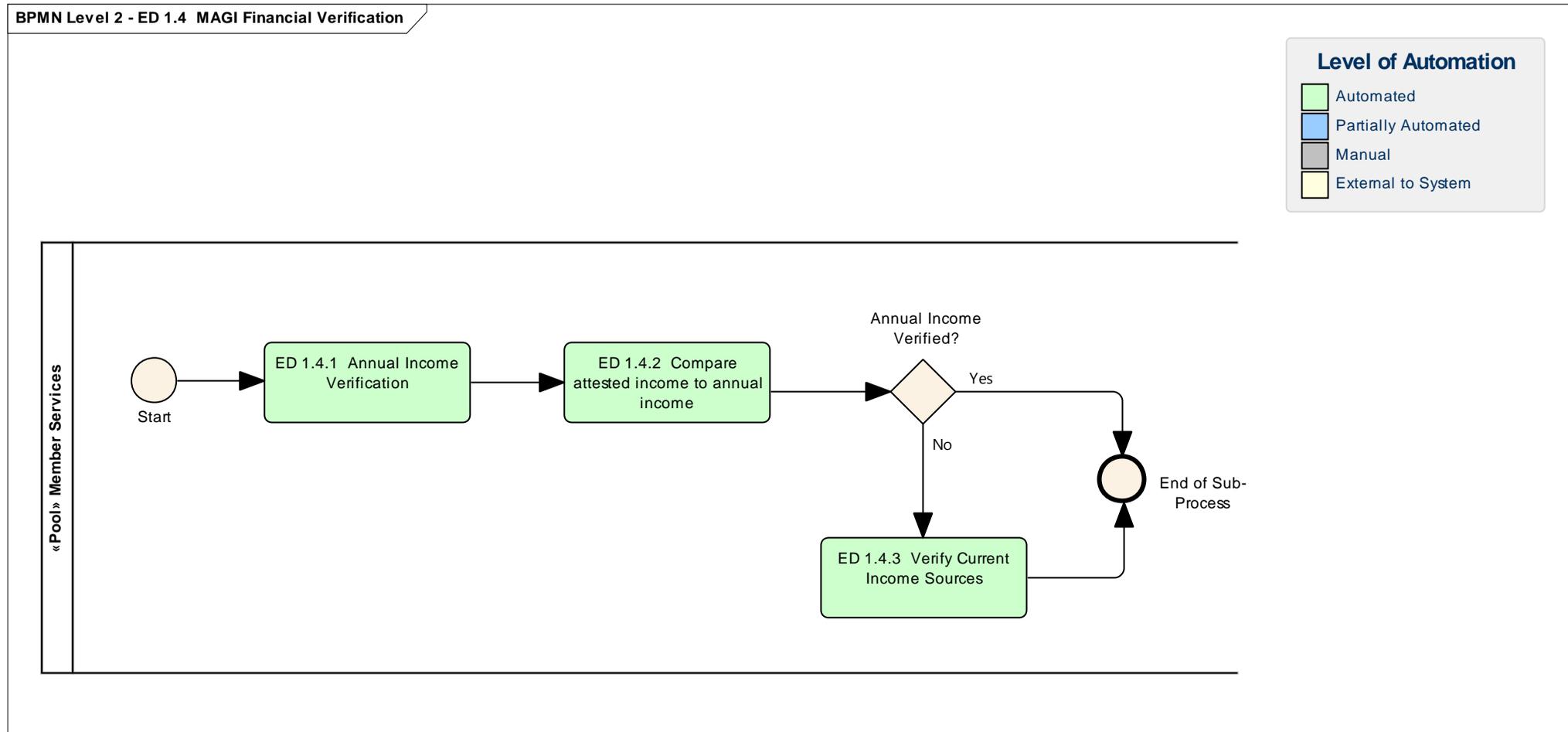


Figure: Level 2: ED 1.7 Request for Verification Notice

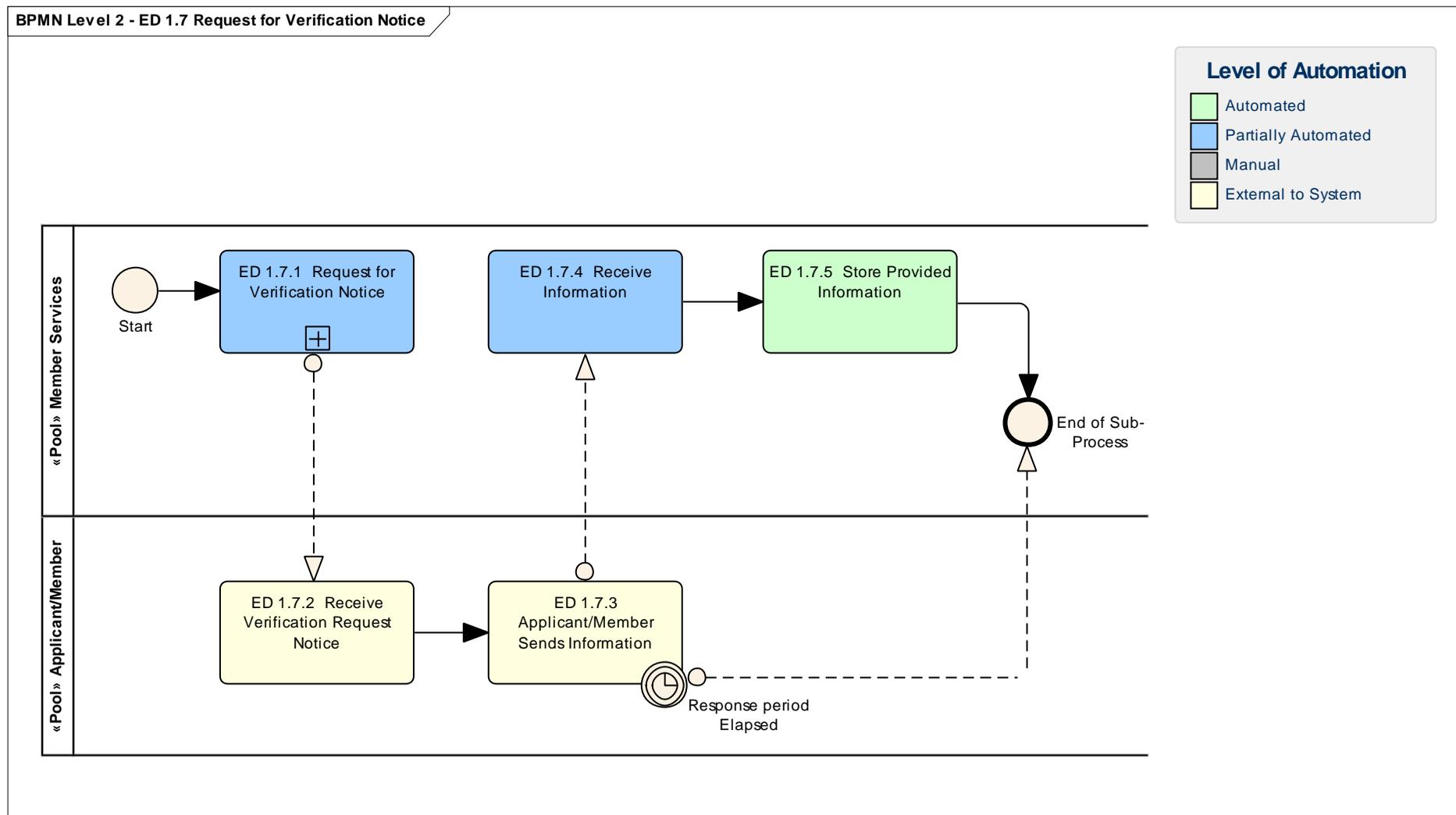


Figure: Level 3: ED 1.7.1 Notices

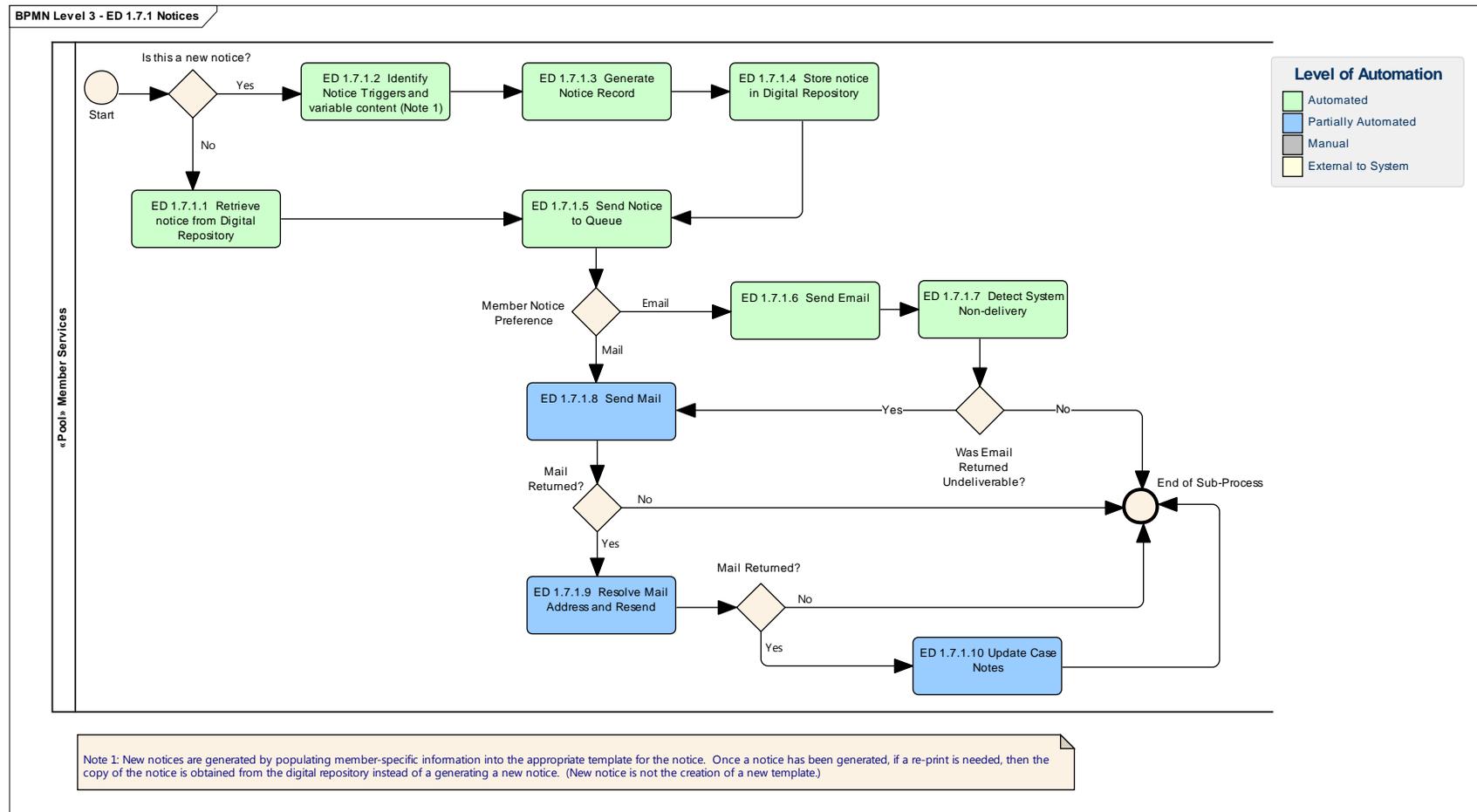


Figure: Level 2: ED 1.8 Eligibility Determination

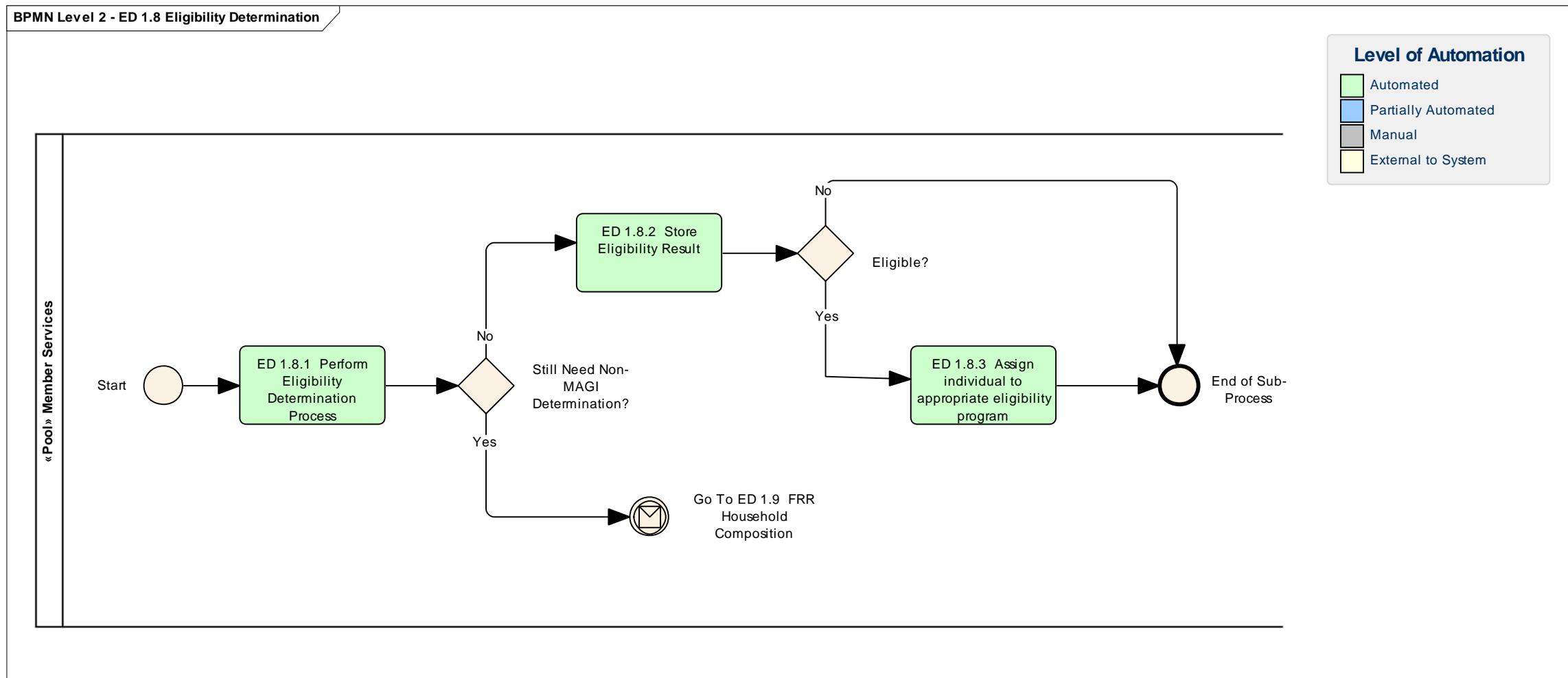


Figure: Level 2: ED 1.10 Non-MAGI Non-Financial Verification

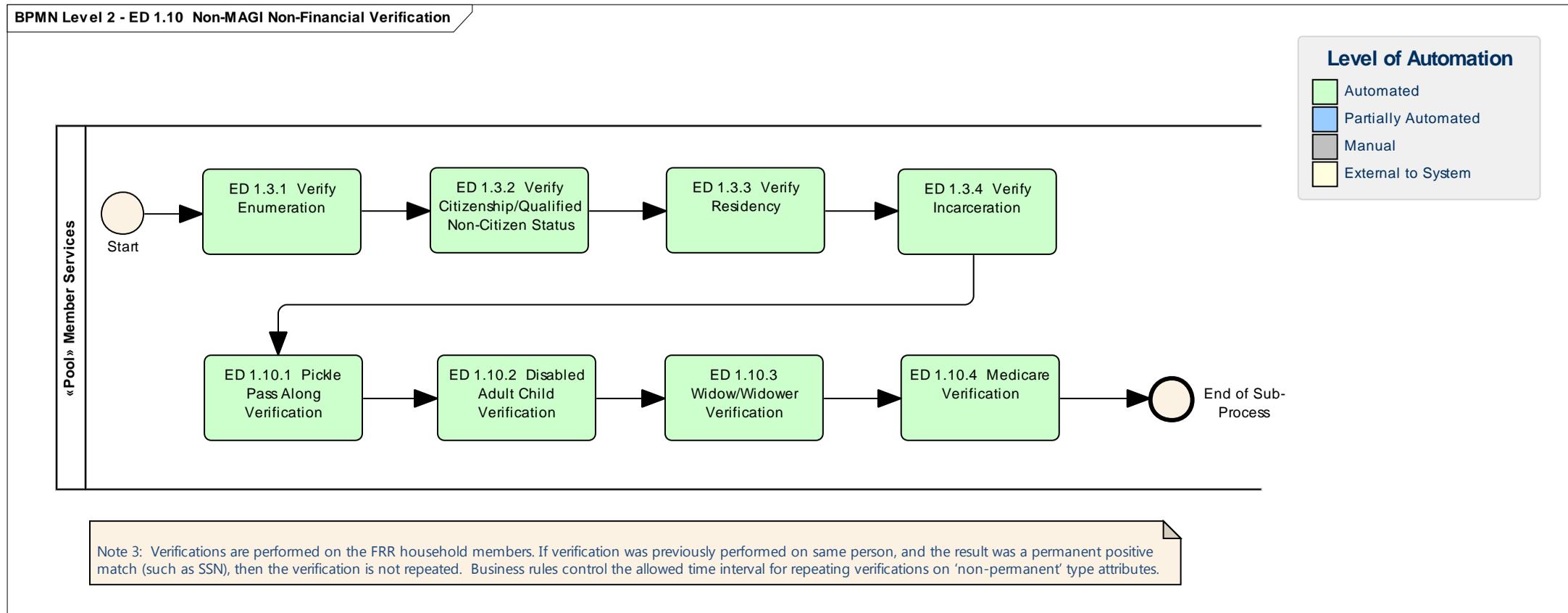


Figure: Level 2: ED 1.11 Non-MAGI Financial Verification

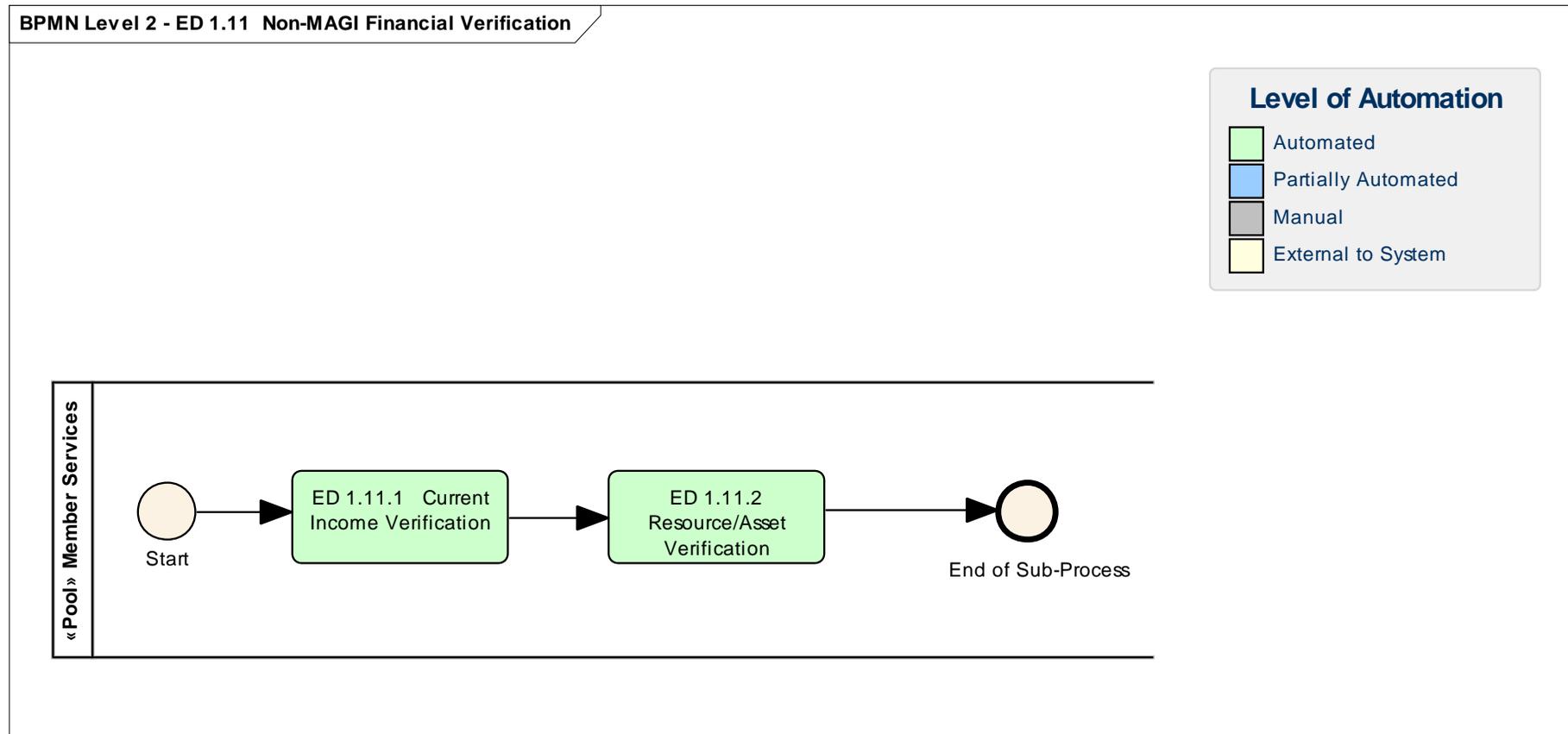


Figure: Level 1: Appeals

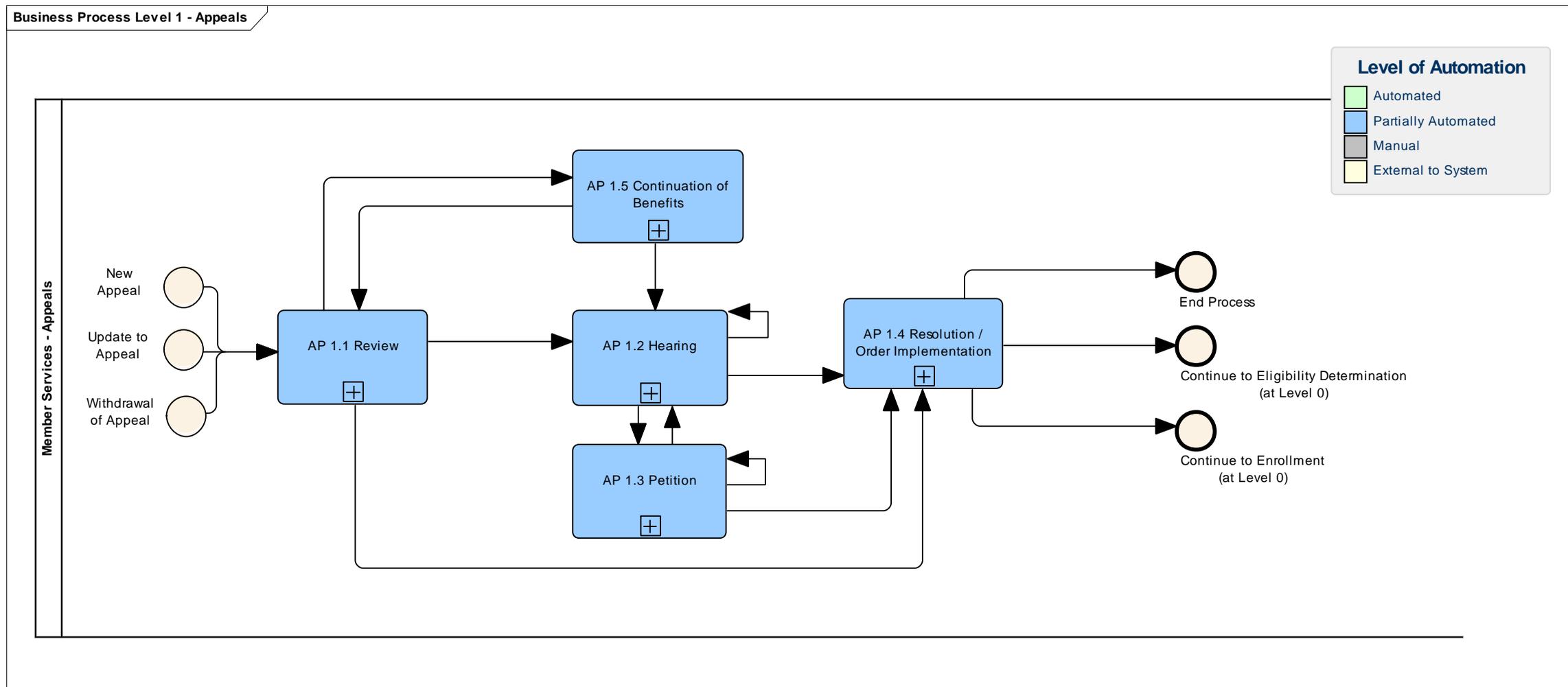


Figure: Level 2: AP 1.1 Review

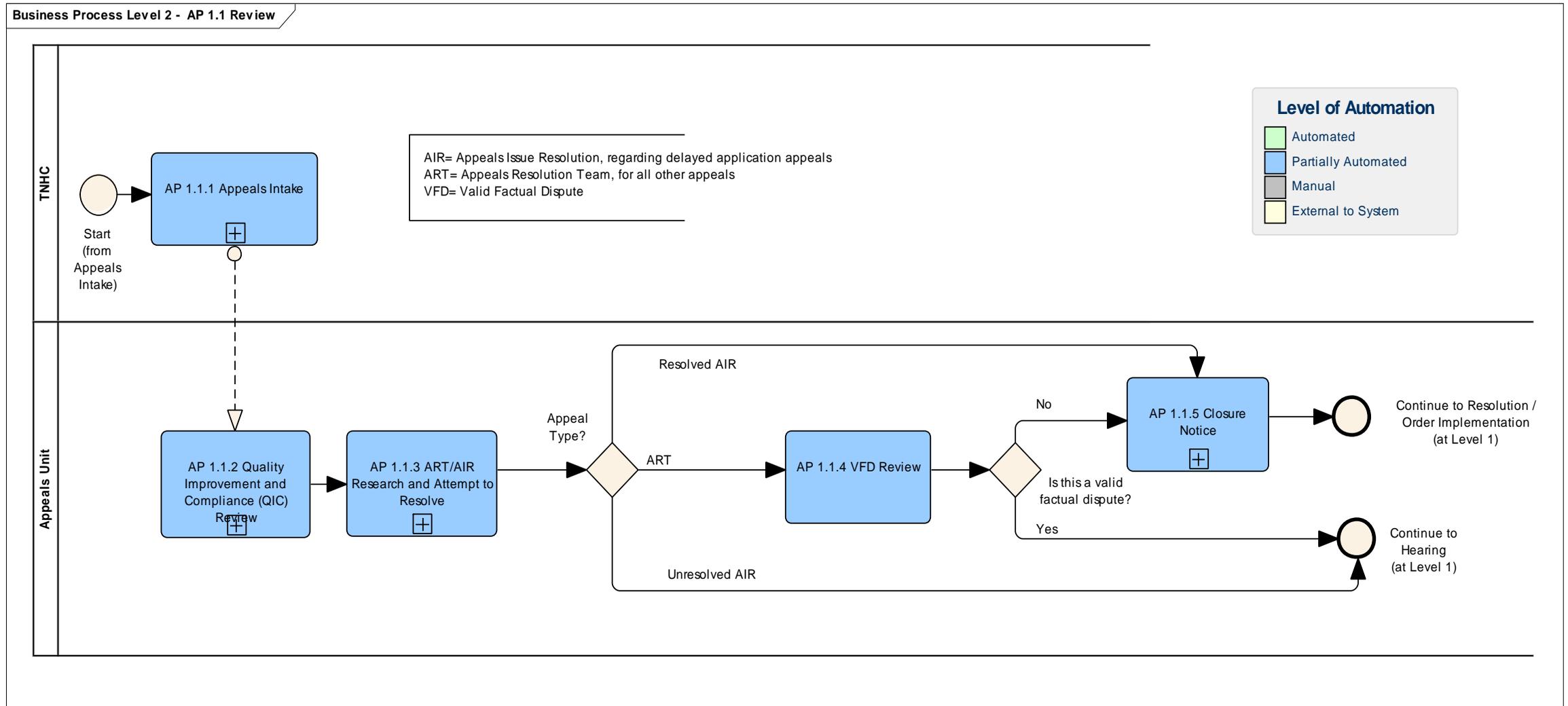


Figure: Level 3: AP 1.1.1 Appeals Intake

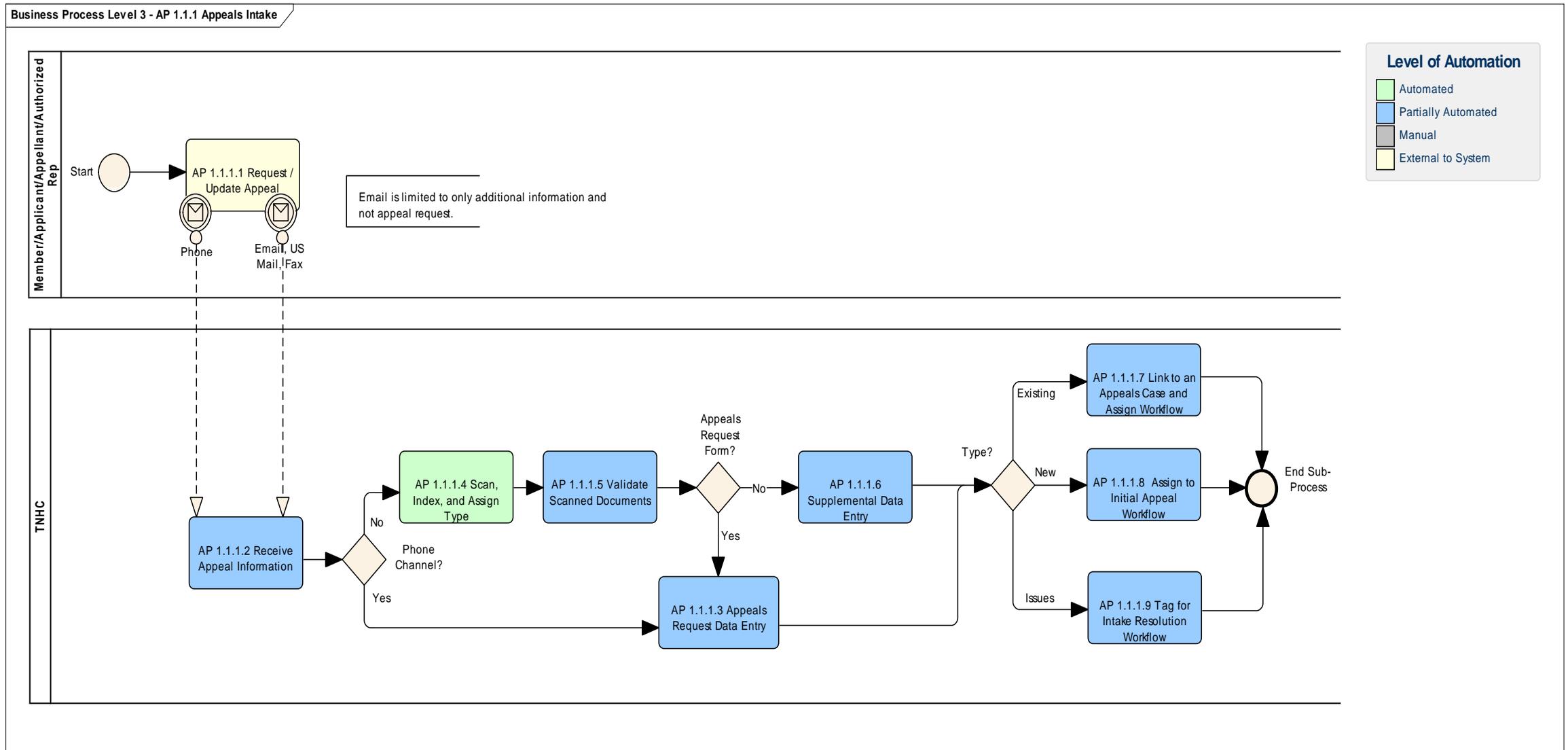


Figure: Level 3: Appeals 1.1.2 Quality Improvement and Compliance Review

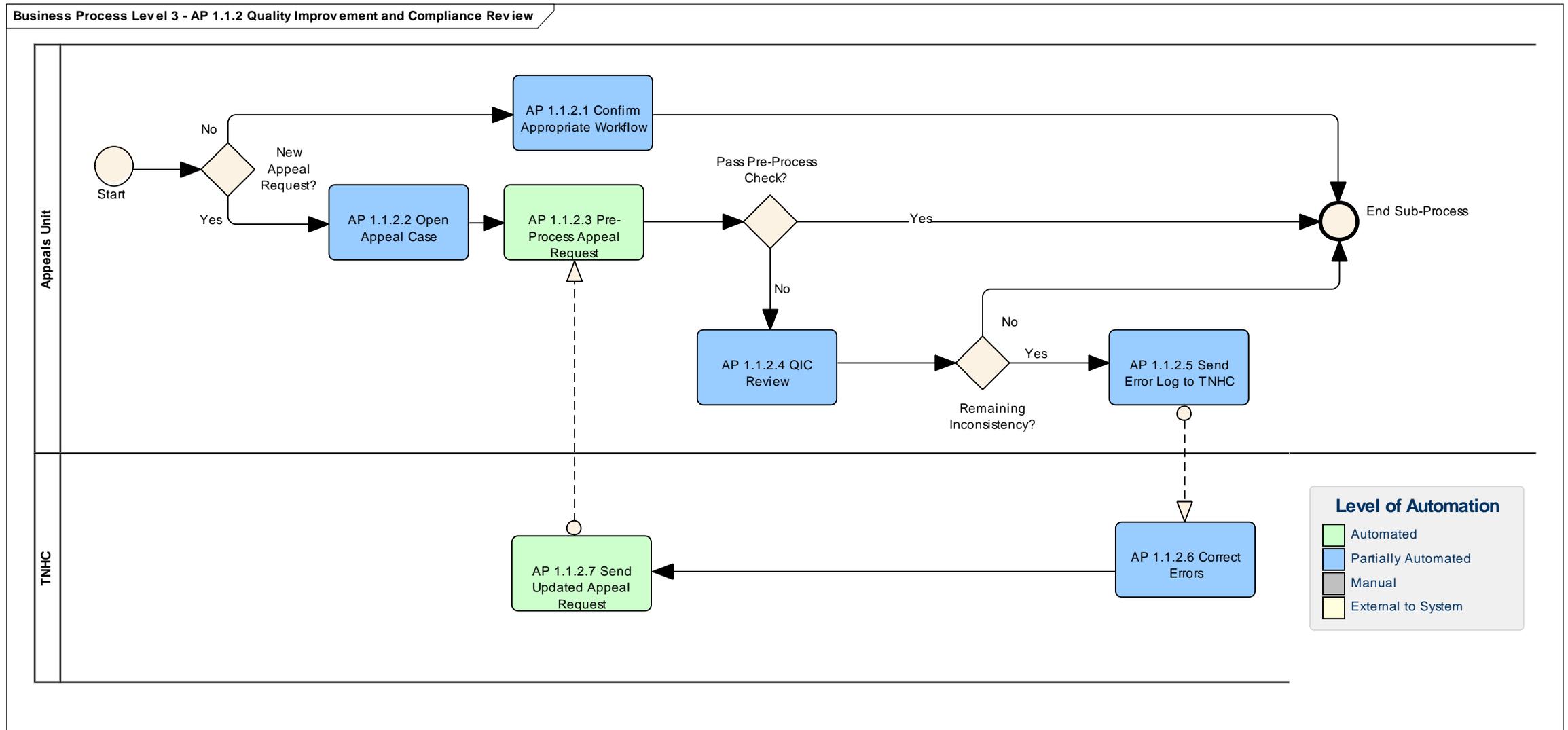


Figure: Level 3: AP 1.1.3 ART/AIR

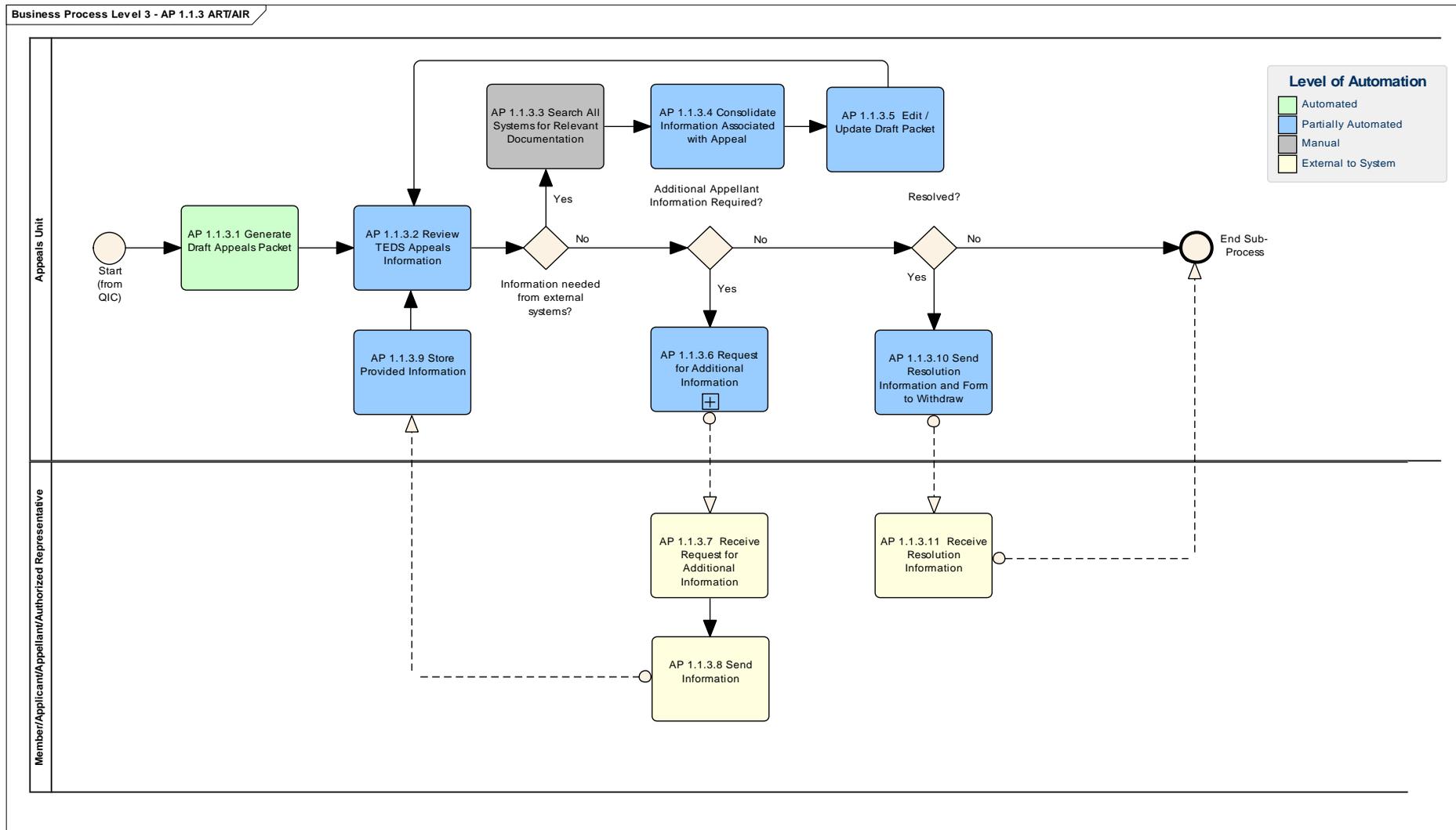


Figure: Level 2: AP 1.2 Hearing

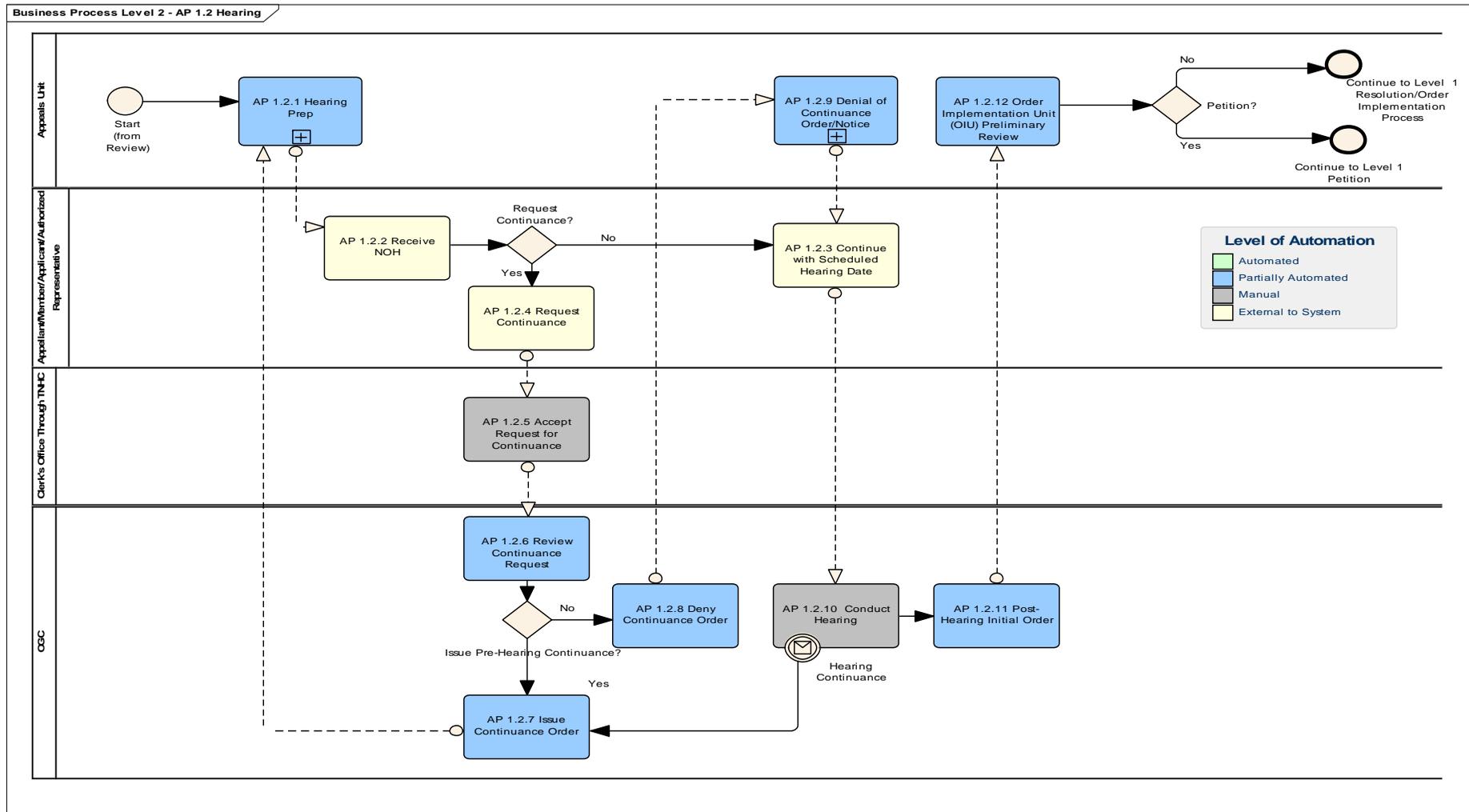


Figure: Level 3: AP 1.2.1 Hearing Prep

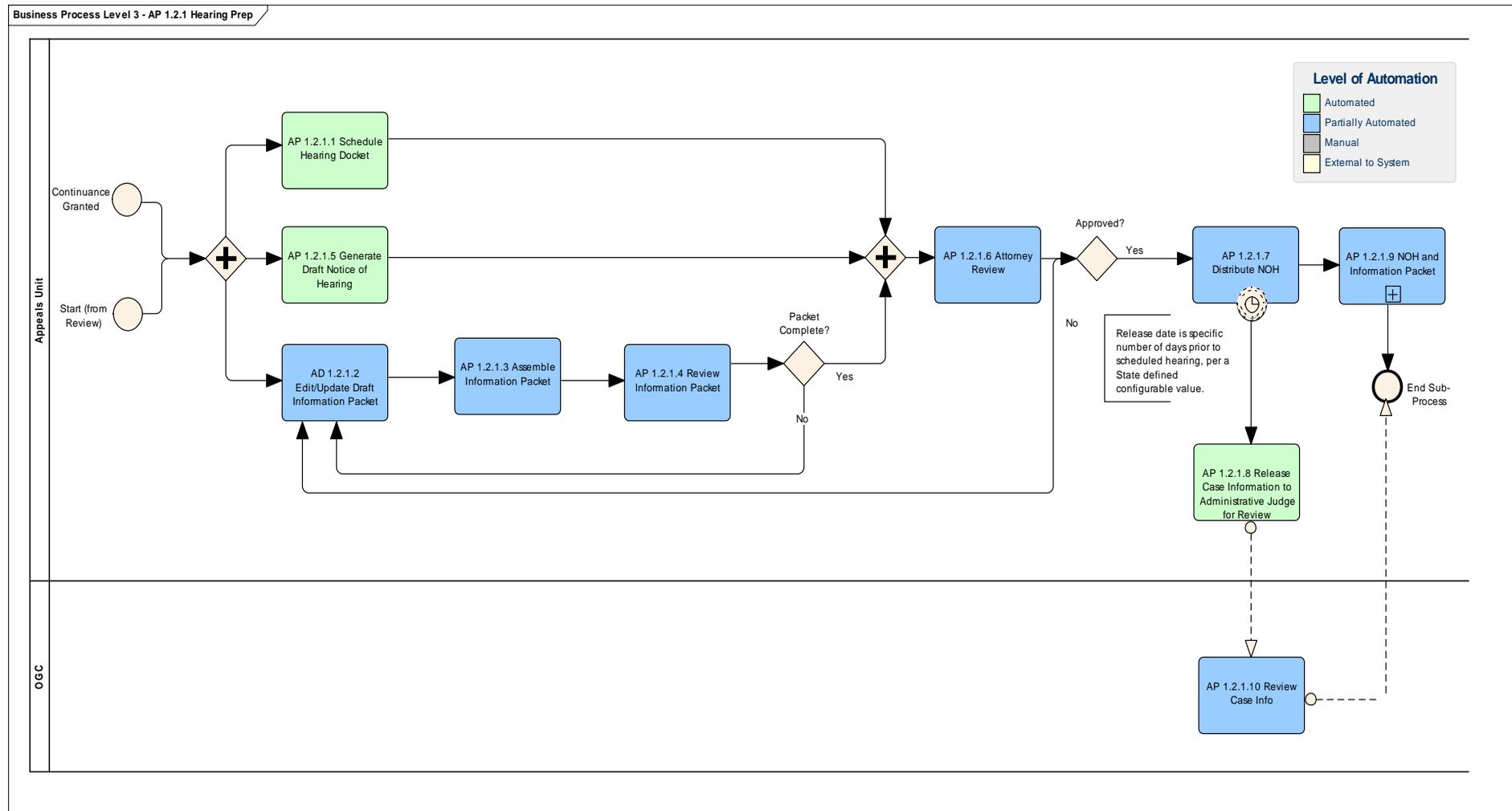


Figure: Level 2: AP 1.3 Petition

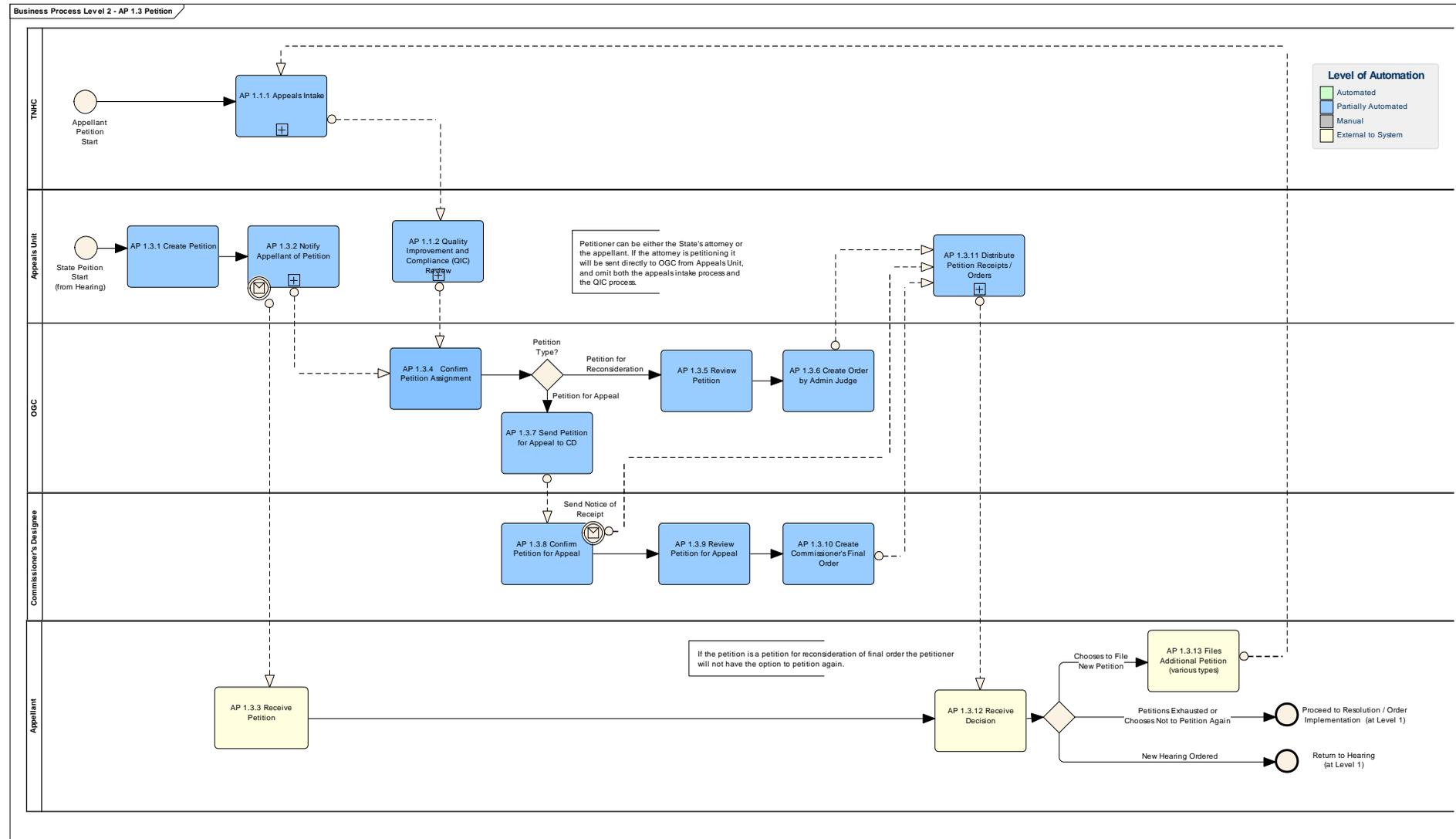


Figure: Level 2: AP 1.4 Resolution/Order Implementation

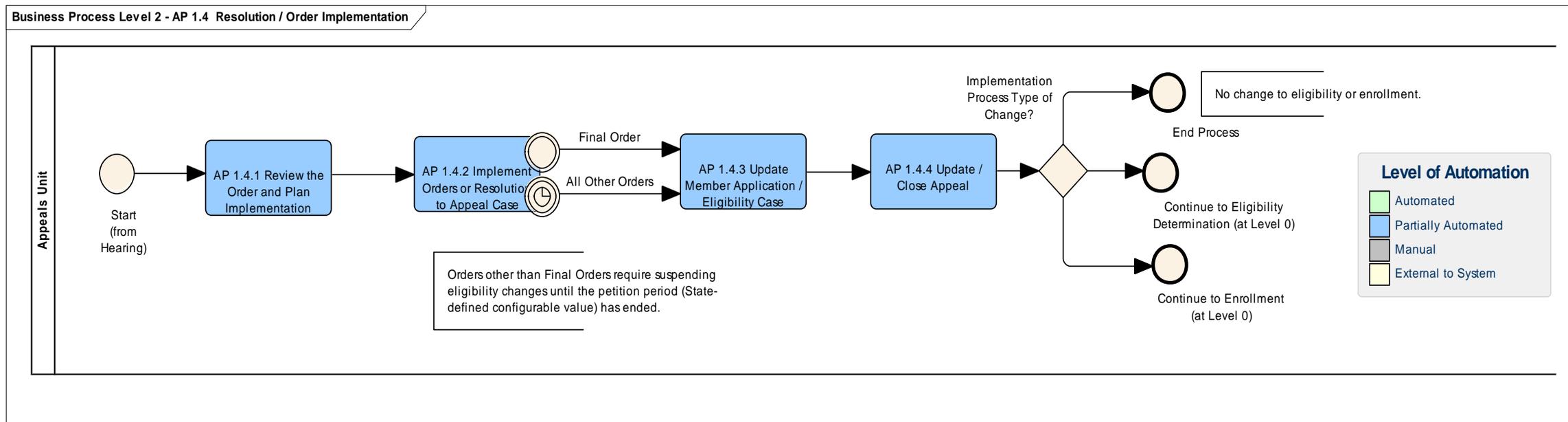


Figure: Level 2: AP 1.5 Continuation of Benefits

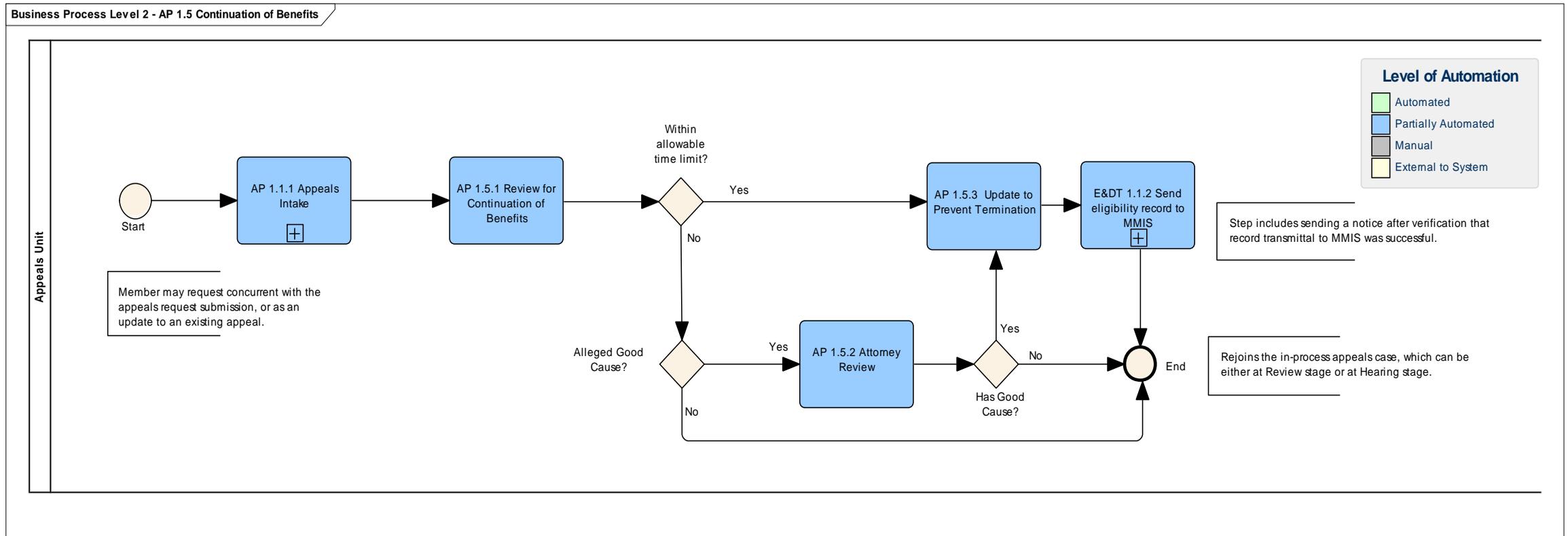


Figure: Level 1: Enrollment & Denial/Termination

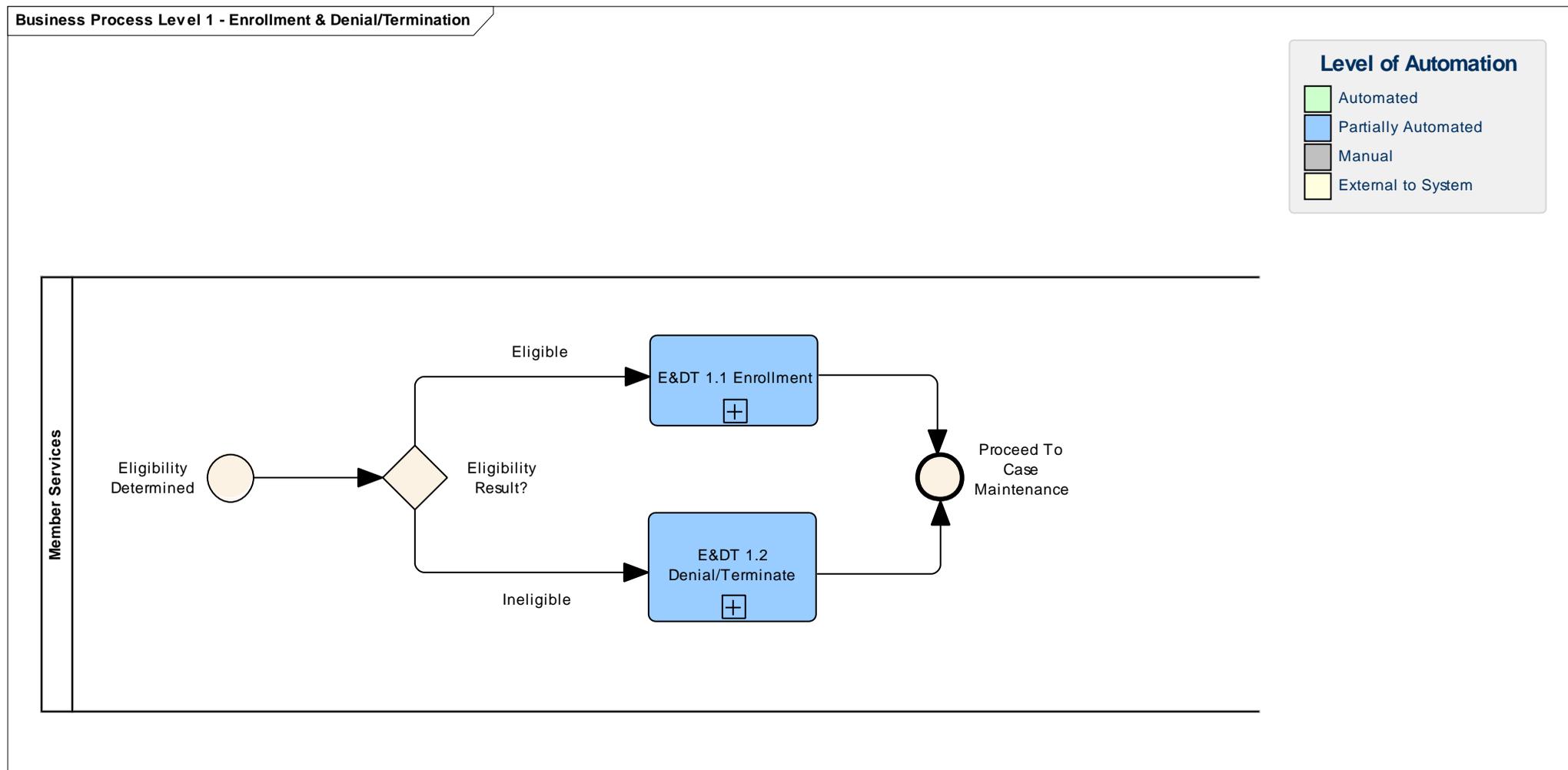


Figure: Level 2: E&DT 1.1 Enrollment

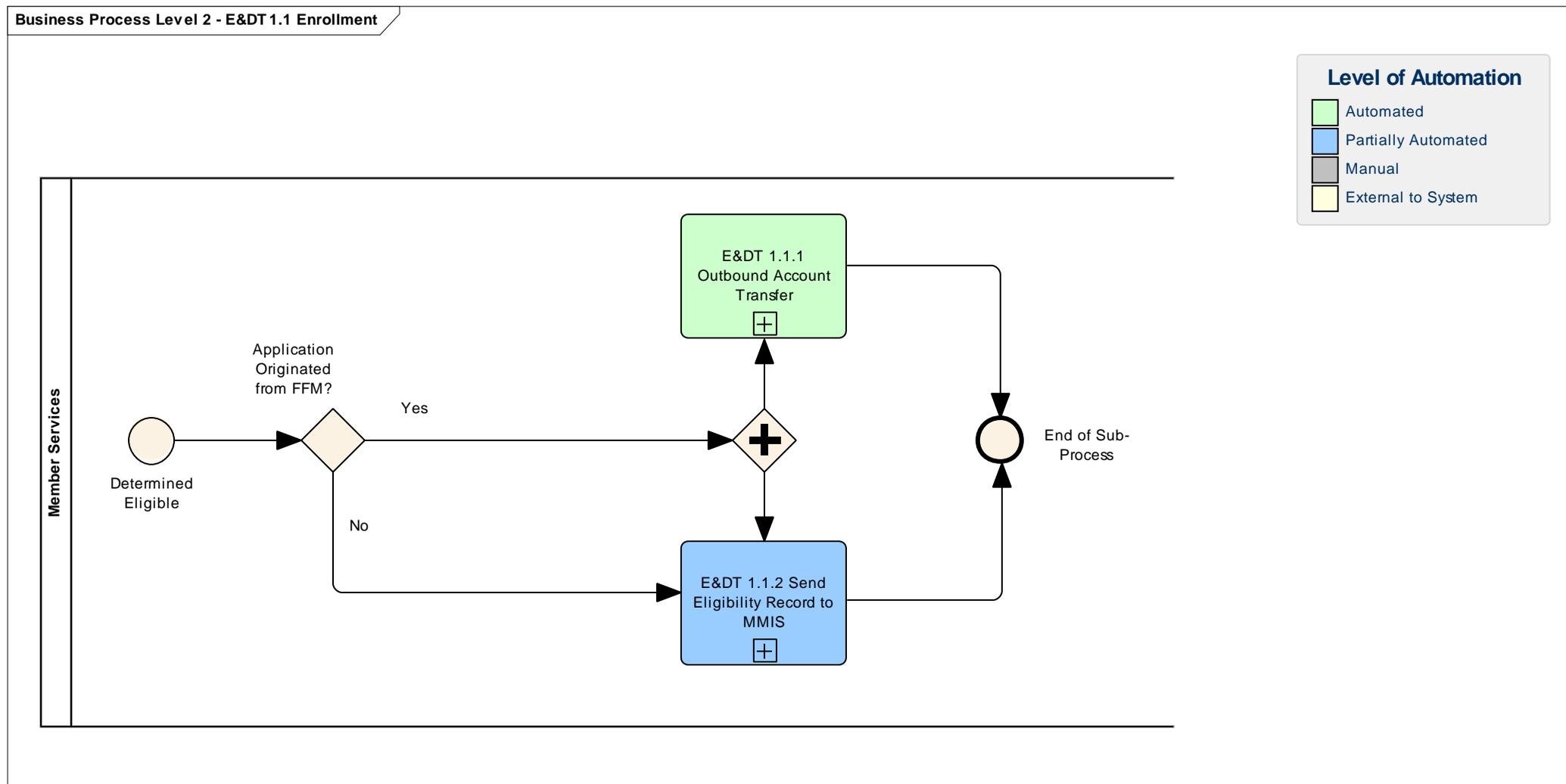


Figure: Level 3: E&DT 1.1.1 Eligibility Information Transfer to External Sources

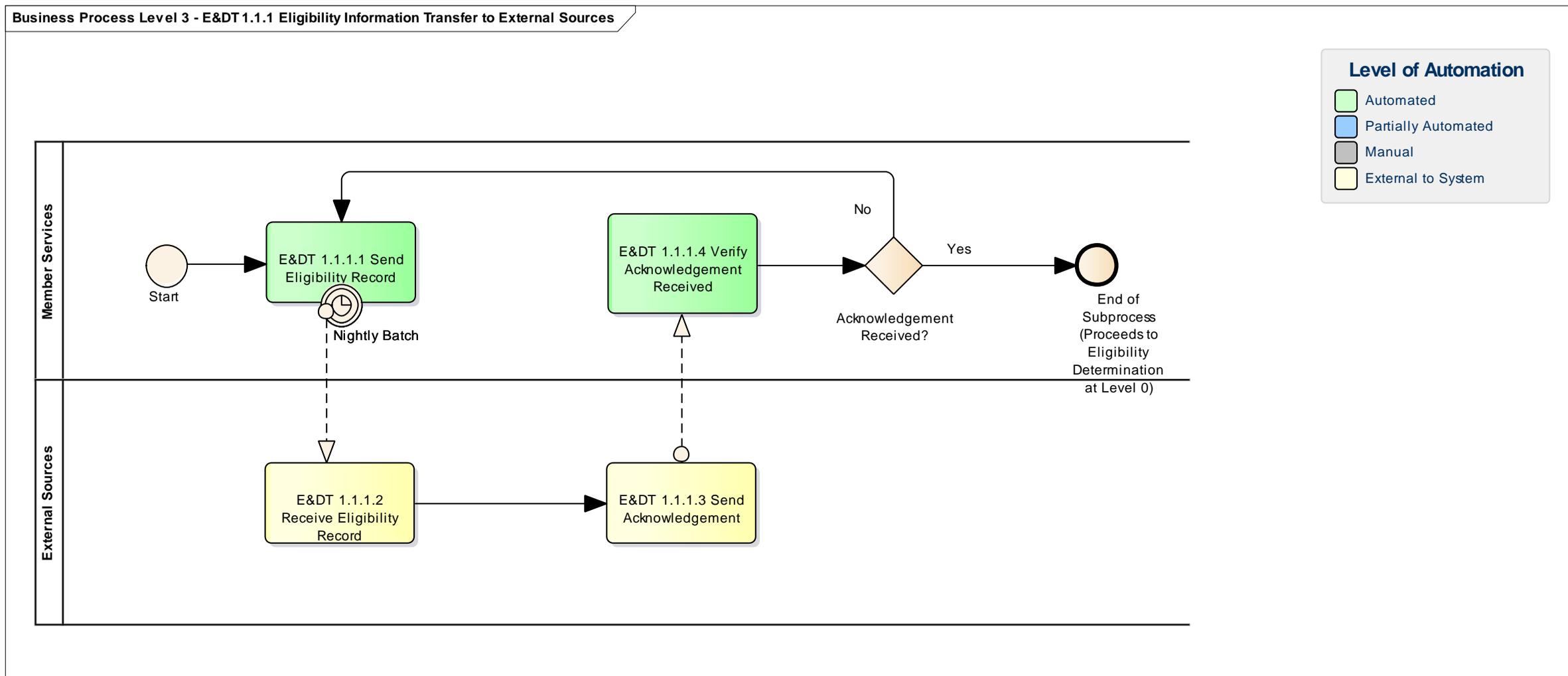


Figure: Level 3: E&DT 1.1.2 Send Eligibility Record to MMIS

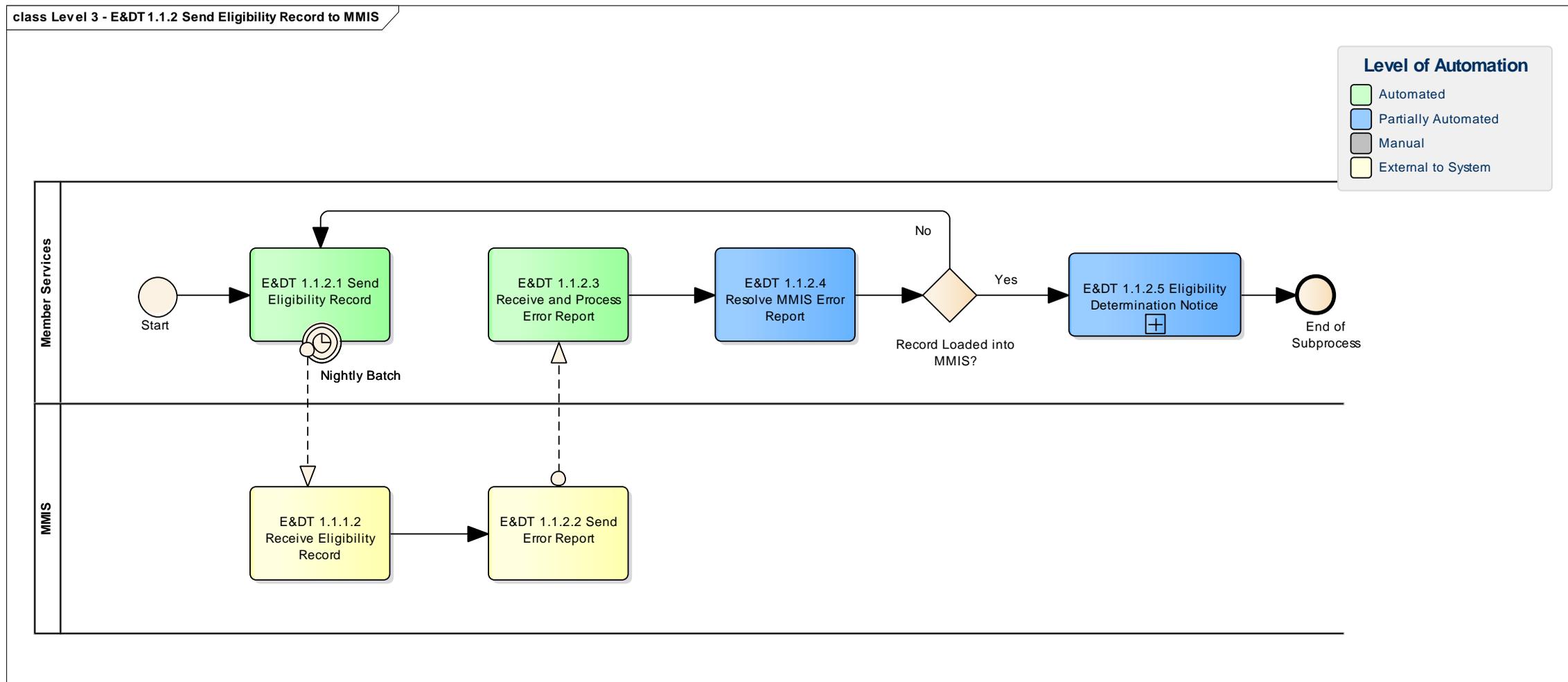


Figure: Level 2: E&DT 1.2 Denial/Terminate

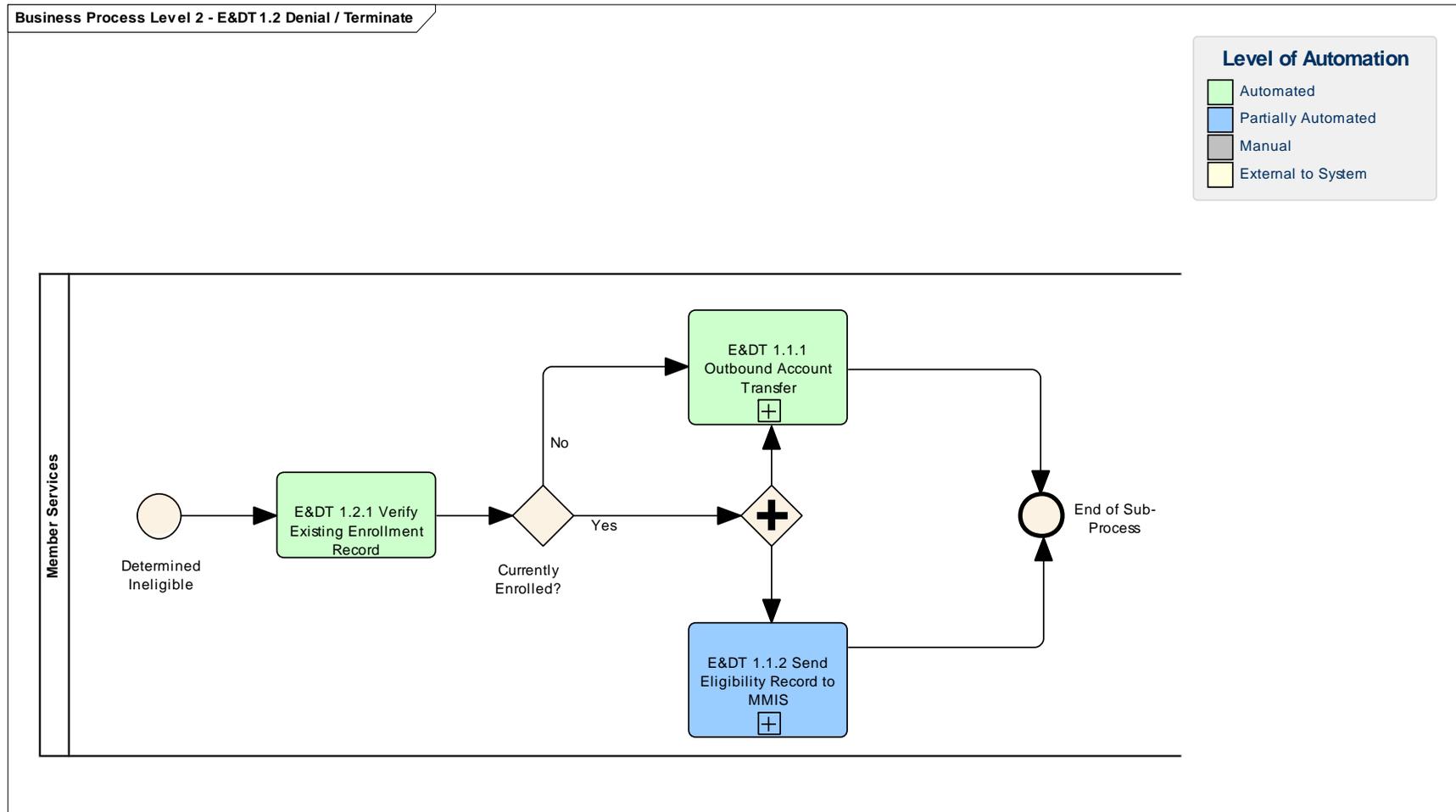


Figure: Level 1: Case Maintenance

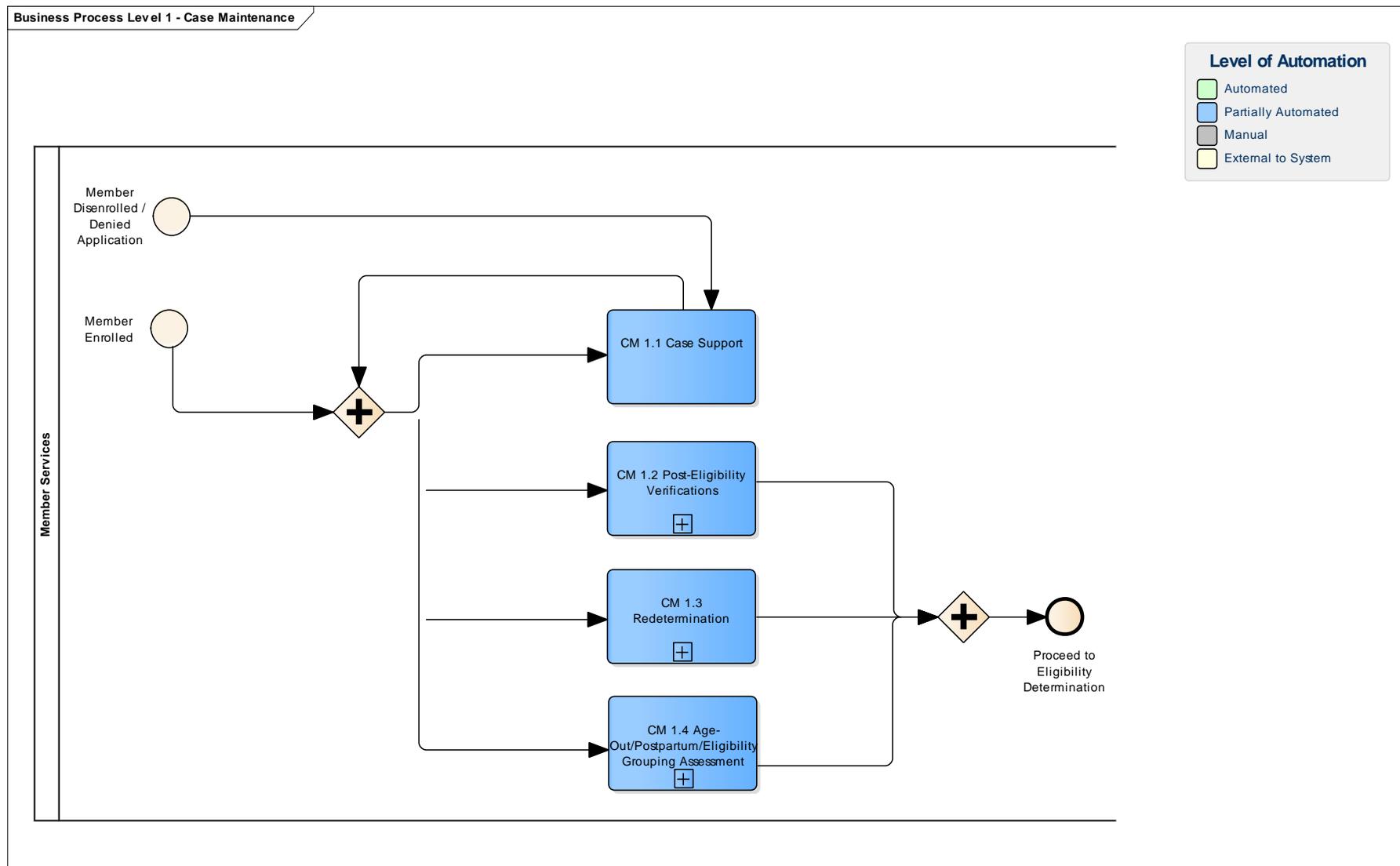


Figure: Level 2: CM 1.2 Post-Eligibility Verifications

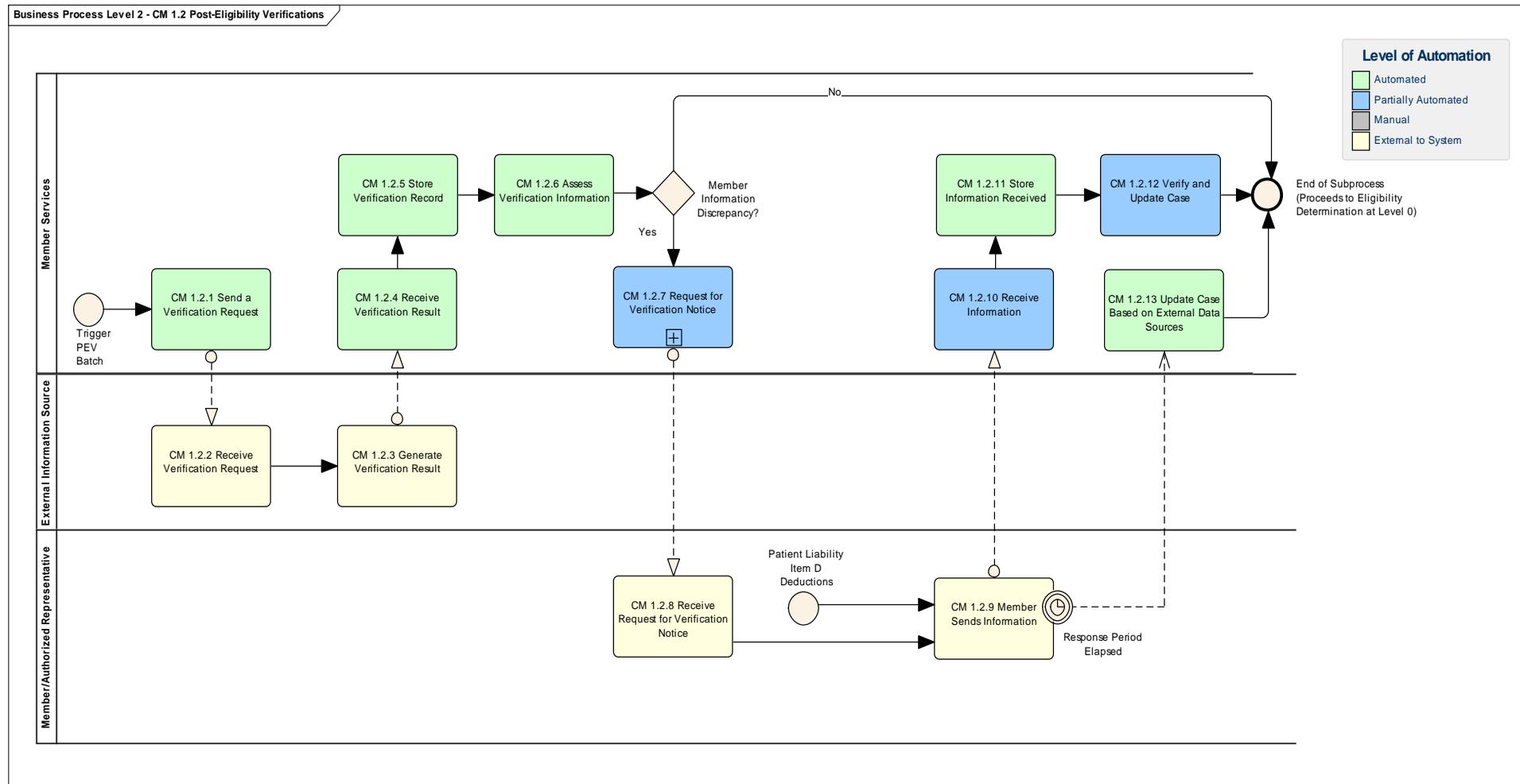


Figure: Level 2: CM 1.3 Redetermination

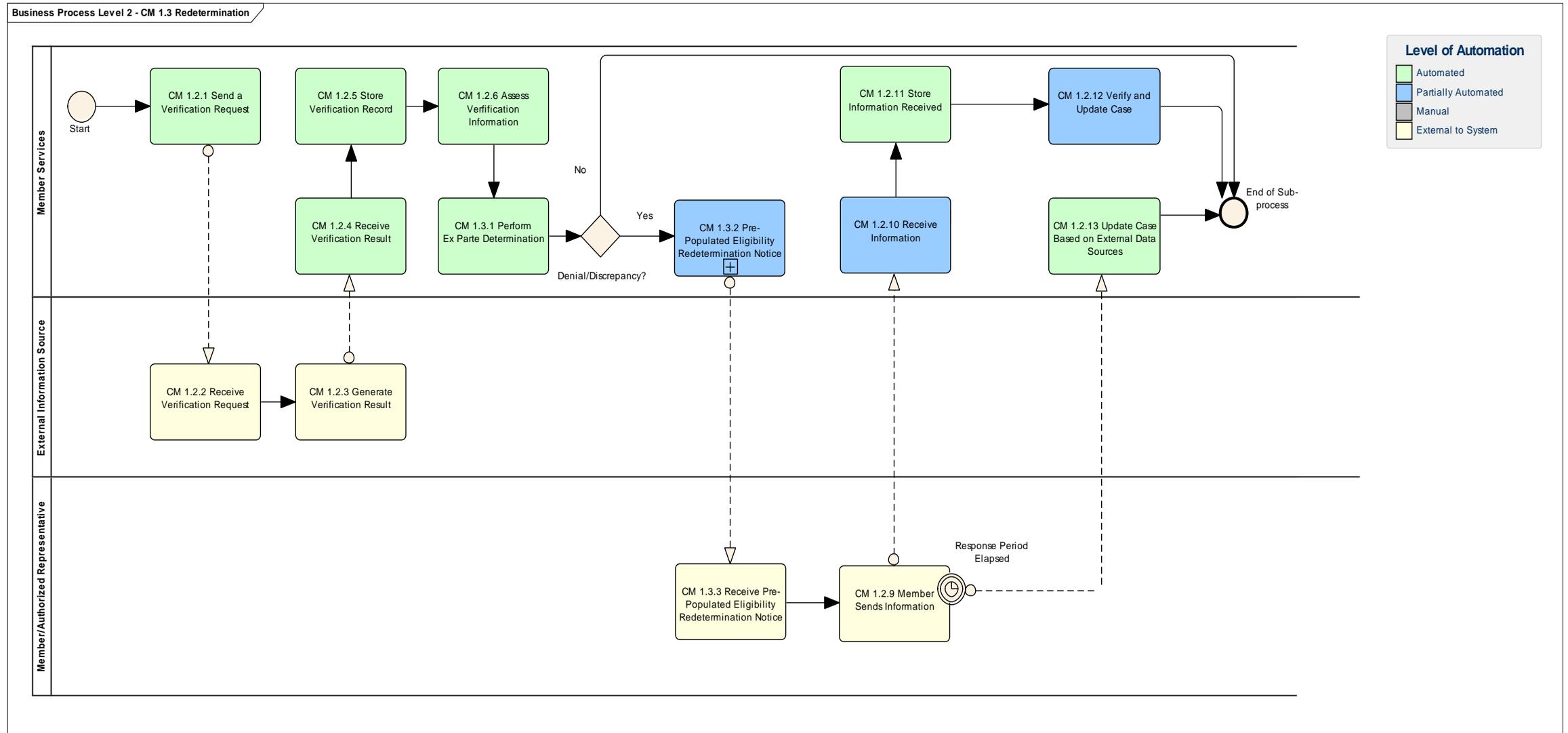
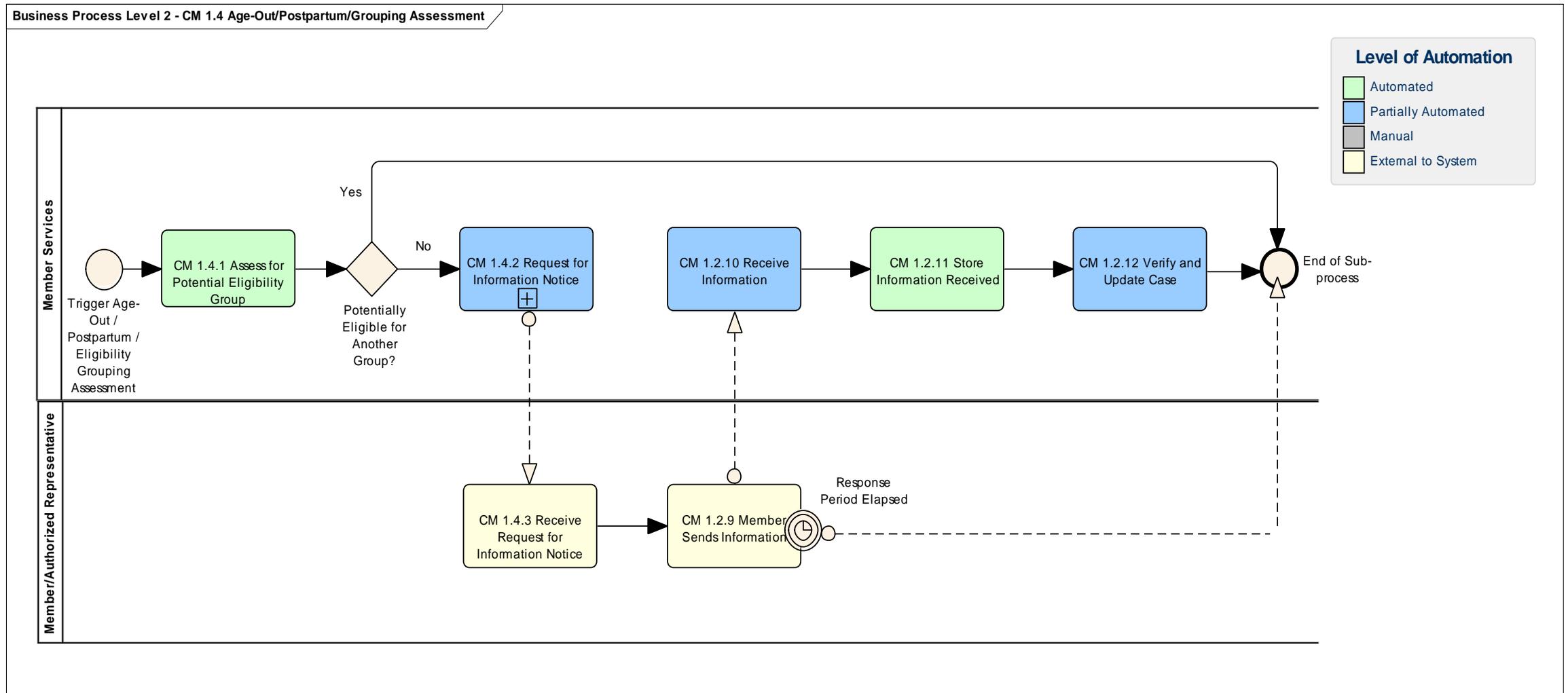


Figure: Level 2: CM 1.4 Age-Out/Postpartum/Grouping Assessment



---

## REQUIREMENTS TRACEABILITY OVERVIEW & MATRIX

### 5.1 Functional Requirements Overview

- 5.1.1 Functional requirements define the expected functionality of the product or system to be created. The State expects the Contractor to describe their approach to designing, developing, and implementing Functional Requirements that supports their Technical Approach to TEDS within a Functional Detailed Design document.
- 5.1.2 The functional requirements for the TEDS are categorized into the sections listed below:
  - 5.1.2.1 Intake - The requirements detail the various channels and pathways that applications shall take within the Solution, the goal of which is to automate processes in order to create efficiencies and maintain a high level of compliant service.
  - 5.1.2.2 Eligibility Determination - The requirements detail a fully automated rules engine that interfaces with the data sources to validate and verify the financial and non-financial information provided and determine eligibility for different programs real-time or near real-time by using the data provided by the applicant.
  - 5.1.2.3 Enrollment, Denial, Redetermination, and Termination - The requirements detail the workflow and interactions needed for the enrollment, denial, redetermination and eligibility termination processes, including communicating these decisions to the applicant and the external sources.
  - 5.1.2.4 Case Maintenance - The requirements detail how the Solution shall facilitate the processes of responding to and resolving inquiries for applicants and beneficiaries.
  - 5.1.2.5 Appeals - The requirements detail how applicants and members shall be able to submit a request for an appeal based on their eligibility determination and to request a hearing. The Solution shall capture information to produce a comprehensive and objective history of the Appeals and Hearings process and all decisions rendered.
  - 5.1.2.6 Alerts - The requirements detail the mechanism to generate and forward notification to internal and external resources.
  - 5.1.2.7 Reports - The requirements detail the mechanisms and methodologies that shall be built to extract relevant information and build reports according to their specifications. The Solution's reporting capabilities are founded on user friendliness and adaptability. It shall produce raw data and polished reports, from the individual- to summary-level, to conform to State and Federal mandates in the present and in the long-term.
  - 5.1.2.8 Workflow Management - The requirements detail how cases and/or tasks shall travel through the Solution from inception to resolution. A case and/or task may require the attention of multiple staff before it is fully completed. The Solution shall ensure that this happens in an expedient manner based on the appropriate hierarchies. The Workflow Management component of the Solution shall help to eliminate redundant work and allow the State to streamline operations.
  - 5.1.2.9 Quality Management - The requirements detail the quality control processes needed for compliance with the state and federal quality standards and to facilitate with the quality audits.

5.1.2.10 Audit - The requirements detail the Solution's capability to store historical information on changes made to data, workflows, and business rules in a viewable audit trail.

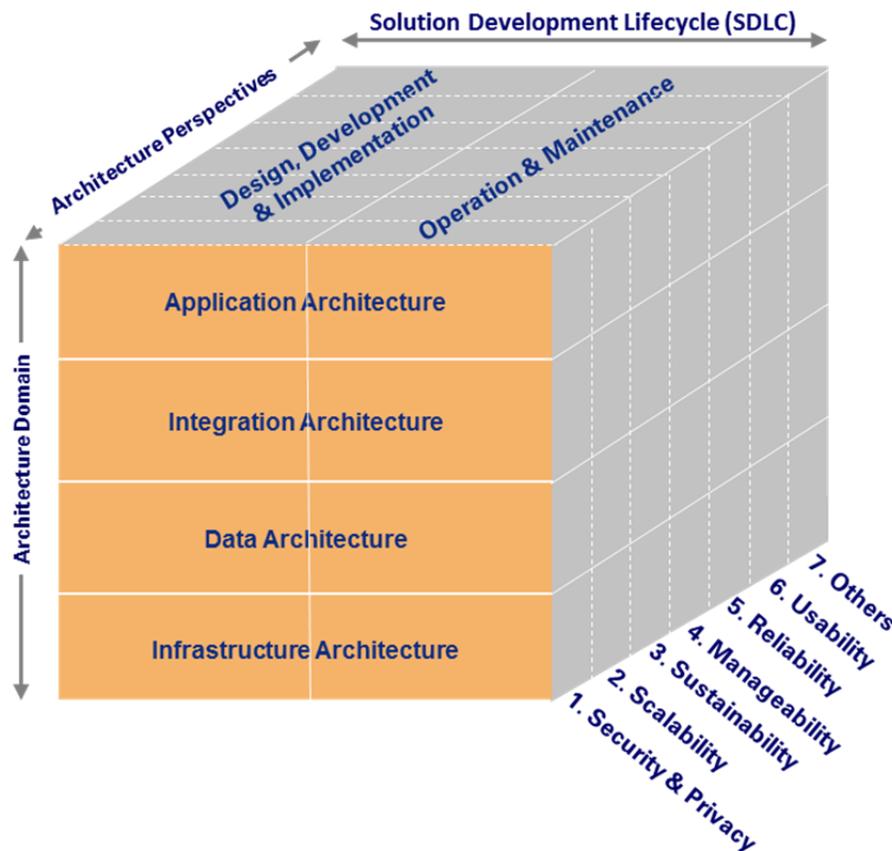
5.1.3 The details of the Functional Requirements for each of these sections are detailed in the Requirement Traceability Matrix, RFQ Attachment J.1. The requirements are also aligned to the process flow/activities of each section.

## 5.2 Technical Requirements Overview

5.2.1 Proposed Ability to Meet State Tennessee Requirements (Non-Functional Requirements)

5.2.1.1 Non-functional Requirements (RFQ Attachment J.2) are defined as those requirements that speak not to the business requirements or the functionality that must be delivered in a Solution but rather the specific technical requirements that must exist in the Solution to deliver the business functionality, the operational objectives and KPIs of the Solution, and the methodology and processes to manage the system delivery and operations. These requirements are illustrated in following three dimensional cube:

Figure: Technical Requirements



5.2.2 As identified in the Figure above, Organization of Non-Functional Requirements, the following categories shall be addressed and expanded upon in the Non-Functional Detailed Design document:

5.2.2.1 Architecture Domains

### 5.2.2.2 Architecture Perspectives

### 5.2.2.3 System Development Lifecycle (SDLC)

5.2.3 Each category has been divided into subcategories as detailed below. Each subcategory has its own tab in the Non-Functional Requirements RTM that is the mandatory RFQ submission.

### 5.2.3.1 Architecture Domains

5.2.3.1.1 Application Architecture - The Application Architecture identifies the Solution's components and the relationships between them to deliver services to stakeholders.

5.2.3.1.2 Integration Architecture - Provision for compliance with interoperability standards such as use of adaptable and open interfaces through an Enterprise Service Bus (ESB) with internal and external systems while implement controls required to protect sensitive data.

5.2.3.1.3 Data Architecture - Data Architecture takes a holistic view of the data used across the Solution with a goal to identify requirements for store, access, movement and management of data to maintain confidentiality, integrity, and availability of data.

5.2.3.1.4 Infrastructure Architecture - Infrastructure Architecture requirements describe the state hosting environments, data centers and disaster recovery configuration to support the Solution. The Contractor needs to navigate the State organizational landscape and coordinates the DDI and operation activities with STS and other service providers to meet the Solution's schedule targets.

### 5.2.3.2 Architecture Perspectives

5.2.3.2.1 Security and Privacy – The security and privacy requirements address the needs to protect privacy and security of member information in accordance with Federal and State regulation and policy mandates (e.g., PPACA, IRS 1075 and HIPAA etc.). The Contractor shall describe the methodology and associated tools required for providing secure system as defined by various Federal and State regulations and policies and industry standards. This includes procedures for system and data security, monitoring and auditing security for breach, identifying, and escalating security incidents. It also includes requirements to secure the privacy of the data as defined by various State and Federal policies and procedures. The requirement provides for the Contractor to supply data classification services for the entire Solution including TEDS data, data from external sources, and upstream/downstream data flows.

5.2.3.2.2 Accessibility – The Contractor shall be responsible for ensuring appropriate Accessibility standards under section 508 of the Rehabilitation Act, WCAG 2.0 AA and Federal civil rights laws are addressed and tested in the proposed Solution.

5.2.3.2.3 Scalability – The Solution will need to be highly scalable and perform to specific standards for different type of transactions and user requests. This includes abilities to scale horizontally and vertically, abilities to monitor system resources and provision additional resources as needed, and abilities to produce systems usage reports to support periodical capacity planning.

5.2.3.2.4 Sustainability – The Solution shall be extensible for ease of maintenance and response to changing future needs and technologies. The Contractor must use conventional technologies that are widely accepted, adopted and are highly interoperable with related systems. The Contractor must include essential actions and resources to ensure the endurance of the Tennessee Medicaid Enterprise. This requires committed leadership, effective governance and the continuity of funding and knowledgeable resources with the critical skills to sustain the architecture.

5.2.3.2.5 Manageability – Systems with a high level of manageability are simpler to deploy, test, and interrogate in the production environment. Highly manageable systems provide the operations team with the right amount of quality information about the state of the service provided, and exhibit predictable and non-catastrophic failure modes when under high load or abnormal conditions, even if those conditions have not before been encountered. Manageable systems lend themselves to rapid diagnosis and simple recovery following a problem, because they have been built with operational criteria as first-class concerns.

5.2.3.2.6 Reliability – The Solution as delivered shall be available and free of technical errors at a level agreed in the contract. The Solution shall meet the recovery time objective (RTO), recovery point objective (RPO) defined in by the State.

5.2.3.2.7 Availability - The Solution as delivered shall be highly available and designed with redundant components and fail-over capabilities. The Solution shall meet the requirements of the State business hours (24/7/365) to support the Member and Worker Portals.

5.2.3.2.8 Usability – Requirements proscribe a highly user friendly system that leverages the UX2014 specification as well as other applicable design principles. All are targeted to achieve the goals below

5.2.3.2.8.1 Intuitive Design and/or user interface

5.2.3.2.8.2 Ease of learning

5.2.3.2.8.3 Efficiency of use

5.2.3.2.8.4 Memorability

5.2.3.2.8.5 Error prevention

5.2.3.2.8.6 User Satisfaction

5.2.4 The details of the Non-Functional Requirements for each of these sections are detailed in the Requirement Traceability Matrix, RFQ Attachment J.2.

**EFFORT WORKBOOK**

---

## OPTIONAL DHS EXPANSION PHASE

### 5.1 Optional Expansion Phase:

- 5.1.1 The State of Tennessee, Department of Human Services (DHS) has begun planning for the modernization and replacement of its legacy information systems necessary to support the Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), Child Care, and Child Support Enforcement programs. This effort has been designated as the DHS Enterprise System Modernization (ESM) project. Refer to Appendix X for a brief description and historical references as to the systems that support each program.
- 5.1.2 Given the age of each system design and/or the dated technology currently used with legacy systems, it is critical for Tennessee to transition toward more efficient, contemporary technology. The DHS ESM vision is to deploy a set of well-integrated systems aligned with and capable of supporting the DHS customer-focused model of practice and integrated delivery of services.
- 5.1.3 The objective of ESM is to provide robust self-service, coordination of DHS services to achieve enhanced efficiencies and effectiveness, and universal workload distribution when and wherever possible. DHS is, therefore, seeking technology that is: 1) current and cost-effective to operate and maintain; 2) fully adaptable and extensible; 2) designed to evolve in response to changes in business conditions, DHS strategies, and regulatory developments; 3) developed to utilize shared technology and business components; and 4) implemented incrementally, in distinct, achievable phases.
- 5.1.4 The Contractor shall incorporate in the design and development of the TEDS such elements of design specifications as shall permit the potential integration of the TEDS with that of the DHS Enterprise System Modernization, currently planned to begin in 2018. Throughout the design, development, and implementation of the Medicaid eligibility system, the Contractor must take into account and prepare for the potential expansion and integration of the system, and ensure that the design of the Medicaid eligibility system provides sufficient flexibility for such expansion.
- 5.1.5 Should the State elect to pursue the Expansion Phase, the State will meet with the Contractor to discuss business and technical requirements for the expanded system and any changes in DDI methodologies related to the Medicaid eligibility system. Based on such information, the Contractor will agree to pricing, which is comparable to pricing, submitted in response to RFQ 32101-15557.
- 5.1.6 For the DDI work, hourly rates and non-labor costs submitted for the DDI work in the Medicaid eligibility system will apply. For the O&M work, rates will align with the rates of the O&M time period in effect for the Medicaid eligibility system.
- 5.1.7 The Expansion Phase will contain modifications to any web portal as required due to take advantage of any lessons learned from the initial implementation. The Expansion Phase may also involve providing access to the Master Person Index (MPI) to other state agencies and merging their existing member rosters with the MPI. The Expansion Phase may also include providing access to the Rules Engine, Enterprise Service Bus, Business Intelligence, and Identify Management to other state agencies.
- 5.1.8 The State shall have sole discretion with regard to pursuing expansion and whether it will engage the Contractor to provide services during the Expansion Phase.

**HIPAA BUSINESS ASSOCIATE AGREEMENT  
HEALTH CARE FINANCE AND ADMINISTRATION  
HIPAA BUSINESS ASSOCIATE AGREEMENT  
IN COMPLIANCE WITH PRIVACY AND SECURITY RULES**

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (“Agreement”) is between **The State of Tennessee, Department of Finance and Administration, Health Care Finance and Administration** (“HCFA” or “Covered Entity”), 310 Great Circle Road, Nashville, TN 37243 and \_\_\_\_\_ (“Business Associate”), located at \_\_\_\_\_, including all office locations and other business locations at which Business Associate data may be used or maintained. Covered Entity and Business Associate may be referred to herein individually as “Party” or collectively as “Parties.”

**BACKGROUND**

The Parties acknowledge that they are subject to the Privacy and Security Rules (45 C.F.R. Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and as amended by the final rule modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (HITECH). If Business Associate provides services to Covered Entity pursuant to one or more contractual relationships, said Agreements are detailed below and hereinafter referred to as “Service Agreements.”

**LIST OF AGREEMENTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT:**

\_\_\_\_\_  
\_\_\_\_\_

In the course of performing services under a Service Agreement, Business Associate may come into contact with, use, or disclose Protected Health Information (“PHI”). Said Service Agreements are hereby incorporated by reference and shall be taken and considered as a part of this document the same as if fully set out herein.

In accordance with the federal privacy and security rules and regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A, C, D and E, which require Covered Entity to have a written memorandum with each of its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI that Business Associate may receive (if any) from or on behalf of Covered Entity, and, therefore, execute this Agreement.

**1. DEFINITIONS**

All capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms defined in 45 C.F.R. Parts 160 through 164 or other applicable law or regulation. A reference

in this Agreement to a section in the Privacy or Security Rule means the section as in effect or as amended.

- 1.1 “Breach of the Security of the [Business Associate’s Information] System” shall mean the unauthorized acquisition, including, but not limited to, access to, use, disclosure, modification or destruction, of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by or on behalf of the Covered Entity under the terms of Tenn. Code Ann. § 47-18-2107 and this Agreement. Good faith acquisition of personal information by an employee or agent of the Information Holder for the purposes of the Information Holder is not a Breach of the Security of the System; provided, that the personal information is not used or subject to further unauthorized disclosure.
- 1.2 “Commercial Use” means obtaining PHI with the intent to sell, transfer or use it for commercial, or personal gain, or malicious harm; sale to third party for consumption, resale, or processing for resale; application or conversion of data to make a profit or obtain a benefit contrary to the spirit of this Agreement, including but not limited to presentation of data or examples of data in a conference or meeting setting where the ultimate goal is to obtain or gain new business.
- 1.3 “Confidential Information” shall mean any non-public, confidential or proprietary information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, which is supplied by HCFA to the Business Associate under this Agreement. Any information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, relating to individuals enrolled in the HCFA program (“HCFA enrollees”), or relating to individuals who may be potentially enrolled in the HCFA program, which is provided to or obtained through the Business Associate’s performance under this Agreement, shall also be treated as “Confidential Information” to the extent that confidential status is afforded such information under state and federal laws or regulations. All confidential information shall not be subject to disclosure under the Tennessee Public Records Act.
- 1.4 “Electronic Signature” means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
- 1.5 “Information Holder” means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information
- 1.6 “Marketing” shall have the meaning under 45 C.F.R. § 164.501 and the act or process of promoting, selling, leasing or licensing any HCFA information or data for profit without the express written permission of HCFA.

## **2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Privacy Rule)**

- 2.1 Compliance with the Privacy Rule. Business Associate shall fully comply with the requirements under the Privacy Rule applicable to "business associates," as that term is defined in the Privacy Rule and not use or further disclose PHI other than as permitted or required by this Agreement, the Service Agreements, or as required by law. In case of any conflict between this Agreement and the Service Agreements, this Agreement shall govern.
- 2.2 HITECH Act Compliance. The Health Information Technology for Economic and Clinical Health Act (HITECH) was adopted as part of the American Recovery and Reinvestment

Act of 2009. HITECH and its implementing regulations impose new requirements on Business Associates with respect to privacy, security, and Breach notification. Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate shall comply with any applicable provisions of HITECH. Business Associate and the Covered Entity further agree that the provisions of HIPAA and HITECH that apply to business associates and that are required to be incorporated by reference in a business associate agreement have been incorporated into this Agreement between Business Associate and Covered Entity. Should any provision not be set forth specifically, it is as if set forth in this Agreement in its entirety and is effective as of the Applicable Effective Date, and as amended.

- 2.3 Business Management. Business Associate may use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate. Business Associate may provide data aggregation services relating to the Health Care Operations of HCFA, or as required by law. Business Associate is expressly prohibited from using or disclosing PHI other than as permitted by this Agreement, any associated Service Agreements, or as otherwise permitted or required by law, and is prohibited from uses or disclosures of PHI that would not be permitted if done by the Covered Entity.
- 2.4 Privacy Safeguards and Policies. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the Service Agreement(s), this Agreement or as required by law. This includes the implementation of Administrative, Physical, and Technical Safeguards to reasonably and appropriately protect the Covered Entity's PHI against any reasonably anticipated threats or hazards, utilizing the technology commercially available to the Business Associate (See also Section 3.2). The Business Associate shall maintain appropriate documentation of its compliance with the Privacy Rule, including, but not limited to, its policies, procedures, records of training and sanctions of members of its Workforce.
- 2.5 Business Associate Contracts. Business Associate shall require any agent, including a Subcontractor, to whom it provides PHI received from, maintained, created or received by Business Associate on behalf of Covered Entity, or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI or other confidential HCFA information, to agree, by written agreement with Business Associate, to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information except for the provision at section 4.6, which shall only apply to the Business Associate notwithstanding the requirements in this section 2.5.
- 2.6 Mitigation of Harmful Effect of Violations. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- 2.7 Reporting of Violations in Use and Disclosure of PHI. Business Associate shall require its employees, agents, and Subcontractors to promptly report to Business Associate immediately upon becoming aware of any use or disclosure of PHI in violation of this Agreement and to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement. The Business Associate shall report such violation to Covered Entity immediately upon becoming aware, and in no case later than 48 hours after discovery.
- 2.8 Breach of Unsecured Protected Health Information. As required by the Breach Notification Rule, Business Associate shall, and shall require its Subcontractor(s) to,

maintain systems to monitor and detect a Breach of Unsecured PHI, whether in paper or electronic form.

2.8.1 Business Associate shall provide to Covered Entity notice of a Breach of Unsecured PHI immediately upon becoming aware of the Breach, and in no case later than 48 hours after discovery.

2.8.2 HCFA shall make the final determination whether the Breach requires notification to affected individuals and whether the notification shall be made by Covered Entity or Business Associate.

2.9 Access of Individual to PHI and other Requests to Business Associate. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to provide access to PHI in a Designated Record Set to Covered Entity in order to meet its requirements under 45 C.F.R. § 164.524. If Business Associate receives a request from an Individual for a copy of the Individual's PHI, and the PHI is in the sole possession of the Business Associate, Business Associate will provide the requested copies to the Individual in a timely manner. If Business Associate receives a request for PHI not in its possession and in the possession of the Covered Entity, or receives a request to exercise other Individual rights as set forth in the Privacy Rule, Business Associate shall promptly forward the request to Covered Entity. Business Associate shall then assist Covered Entity as necessary in responding to the request in a timely manner. If a Business Associate provides copies of PHI to the Individual, it may charge a reasonable fee for the copies as the regulations shall permit.

2.10 Requests to Covered Entity for Access to PHI. The Covered Entity shall forward to the Business Associate in a timely manner any Individual's request for access to or a copy (in any form they choose, provided the PHI is readily producible in that format) of their PHI that shall require Business Associate's participation, after which the Business Associate shall provide access to or deliver such information as follows:

- a) The Parties understand that if either Party receives a request for access to or copies of PHI from an Individual which the Party may complete with only its own onsite information, the time for such response shall be thirty (30) days, with notification to the Covered Entity upon completion.
- b) If Covered Entity does not have the requested PHI onsite and directs Business Associate to provide access to or a copy of his/her PHI directly to the Individual, or Individual's designee, the Business Associate shall have sixty (60) days from the date of the Individual's request to provide access to PHI or deliver a copy of such information to the Individual. The Business Associate shall notify the Covered Entity when it completes the response.
- c) If the Covered Entity receives a request and requires information from the Business Associate in addition to the Covered Entity's onsite information to fulfill the request, the Business Associate shall have thirty (30) days from date of Covered Entity's notice to provide access or deliver such information to the Covered Entity so that the Covered Entity may timely respond to the Individual within the sixty (60) day requirement of 45 C.F.R. § 164.524.
- d) If the Party designated above as responding to the Individual's request is unable to complete the response to the request in the time provided, that Party shall provide the Individual, or Individual's designee, with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Party may extend the response time once for no more than thirty (30) additional days.

- e) Business Associates permitted to send an Individual or Individual's designee unencrypted emails including Electronic PHI if the Individual requests it, provided the Business Associate has advised the Individual of the risk and the Individual still prefers to receive the message by unencrypted email.
  - f) Business Associate shall develop forms that are designed to collect the necessary written, signed designation that is required in order to permit Individuals to designate recipients of PHI.
- 2.11 Individuals' Request to Amend PHI. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526, regarding an Individual's request to amend PHI. The Business Associate shall make the amendment promptly in the time and manner designated by Covered Entity, but shall have thirty (30) days' notice from Covered Entity to complete the amendment to the Individual's PHI and to notify the Covered Entity upon completion.
- 2.12 Recording of Designated Disclosures of PHI. Business Associate shall document any and all disclosures of PHI by Business Associate or its agents, including information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.
- 2.13 Accounting for Disclosures of PHI. The Business Associate agrees to provide to Covered Entity or to an Individual, or Individual's designee, in time and manner designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. The Covered Entity shall forward the Individual's request requiring the participation of the Business Associate to the Business Associate in a timely manner, after which the Business Associate shall provide such information as follows:
- a) If Covered Entity directs Business Associate to provide an accounting of disclosures of the Individual's PHI directly to the Individual, the Business Associate shall have sixty (60) days from the date of the Individual's request to provide access to or deliver such information to the Individual or Individual's designee. The Covered Entity shall provide notice to the Business Associate in time to allow the Business Associate a minimum of thirty (30) days to timely complete the Individual's request.
  - b) If the Covered Entity elects to provide the accounting to the Individual, the Business Associate shall have thirty (30) days from date of Covered Entity's notice of request to provide information for the Accounting to the Covered Entity so that the Covered Entity may timely respond to the Individual within the sixty (60) day period.
  - c) If either of the Parties is unable to complete the response to the request in the times provided above, that Party shall notify the Individual with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Parties may extend the response time once for no more than thirty (30) additional days.
  - d) The accounting of disclosures shall include at least the following information:
    - 1) date of the disclosure;
    - 2) name of the third party to whom the PHI was disclosed,

- 3) if known, the address of the third party;
  - 4) brief description of the disclosed information; and
  - 5) brief explanation of the purpose and basis for such disclosure.
    - e) The Parties shall provide one (1) accounting in any twelve (12) months to the Individual without charge. The Parties may charge a reasonable, cost-based fee, for each subsequent request for an accounting by the same Individual if he/she is provided notice and the opportunity to modify his/her request. Such charges shall not exceed any applicable State statutes or rules.
- 2.14 Minimum Necessary. Business Associate shall to use reasonable efforts to limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.
- 2.14.1 Business Associate represents to Covered Entity that all its uses and disclosures of, or requests for, PHI shall be the minimum necessary in accordance with the Privacy Rule requirements.
- 2.14.2 Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate.
- 2.14.3 Business Associate shall adequately and properly maintain all PHI received from, or created or received on behalf of, Covered Entity.
- 2.15 Privacy Compliance Review upon Request. Business Associate agrees to make its internal practices, books and records, including policies, procedures, and PHI, relating to the use and disclosure of PHI received from, created by or received by Business Associate on behalf of Covered Entity available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.
- 2.16 Cooperation in Privacy Compliance. Business Associate agrees to fully cooperate in good faith and to assist Covered Entity in complying with the requirements of the Privacy Rule.

### **3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Security Rule)**

- 3.1 Compliance with Security Rule. Business Associate shall fully comply with the requirements under the Security Rule applicable to "Business Associates," as that term is defined in the Security Rule. In case of any conflict between this Agreement and Service Agreements, this Agreement shall govern.
- 3.2 Security Safeguards and Policies. Business Associate shall implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule. This includes specifically, but is not limited to, the utilization of technology commercially available at the time to the Business Associate to protect the Covered Entity's PHI against any reasonably anticipated threats or hazards. The Business Associate understands that it has an affirmative duty to perform a regular review or assessment of

security risks, conduct active risk management and supply best efforts to assure that only authorized persons and devices access its computing systems and information storage, and that only authorized transactions are allowed. The Business Associate will maintain appropriate documentation of its compliance with the Security Rule.

- 3.3 Security Provisions in Business Associate Contracts. Business Associate shall ensure that any agent to whom it provides Electronic PHI received from, maintained, or created for Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, shall execute a bilateral contract (or the appropriate equivalent if the agent is a government entity) with Business Associate, incorporating the same restrictions and conditions in this Agreement with Business Associate regarding PHI except for the provision in Section 4.6.
- 3.4 Tennessee Consumer Notice of System Breach. Business Associate understands that the Covered Entity is an "Information Holder" (as may be Business Associate) under the terms of Tenn. Code Ann. § 47-18-2107, and that in the event of a breach of the Business Associate's security system as defined by that statute and Definition 1.1 of this agreement, the Business Associate shall indemnify and hold the Covered Entity harmless for expenses and/or damages related to the breach. Such obligation shall include, but is not limited to, the mailed notification to any Tennessee resident whose personal information is reasonably believed to have been acquired by an unauthorized individual. In the event that the Business Associate discovers circumstances requiring notification of more than one thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution and content of the notices. Substitute notice, as defined by Tenn. Code Ann. § 47-18-2107(e)(2) and (3), shall not be permitted except as approved in writing in advance by the Covered Entity. The parties agree that PHI includes data elements in addition to those included by "personal information" under Tenn. Code Ann. § 47-18-2107, and agree that Business Associate's responsibilities under this paragraph shall include all PHI.
- 3.5 Reporting of Security Incidents. The Business Associate shall track all Security Incidents as defined by HIPAA and shall periodically report such Security Incidents in summary fashion as may be requested by the Covered Entity, but not less than annually within sixty (60) days of the anniversary of this Agreement. The Covered Entity shall not consider as Security Incidents, for the purpose of reporting, external activities (port enumeration, etc.) typically associated with the "footprinting" of a computing environment as long as such activities have only identified but not compromised the logical network perimeter, including but not limited to externally facing firewalls and web servers. The Business Associate shall reasonably use its own vulnerability assessment of damage potential and monitoring to define levels of Security Incidents and responses for Business Associate's operations. However, the Business Associate shall expediently notify the Covered Entity's Privacy Officer of any Security Incident, including any "breach of the security of the system" under Tenn Code Ann. § 47-18-2107, immediately upon becoming aware of any unauthorized acquisition including but not limited to use, disclosure, modification, or destruction of PHI by an employee or otherwise authorized user of its system of which it becomes aware.
- 3.5.1 Business Associate identifies the following key contact persons for all matters relating to this Agreement:

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

---



---

Business Associate shall notify Covered Entity of any change in these key contacts during the term of this Agreement in writing within ten (10) business days.

- 3.6 Contact for Security Incident Notice. Notification for the purposes of Sections 2.9, 3.4 and 3.5 shall be in writing made by email/fax, certified mail or overnight parcel immediately upon becoming aware of the event, with supplemental notification by facsimile and/or telephone as soon as practicable, to:
- Privacy Officer  
HCFA  
310 Great Circle Rd.  
Nashville Tennessee 37243  
Phone: (615) 507-6855 Facsimile: (615) 532-7322
- 3.7 Security Compliance Review upon Request. Business Associate shall make its internal practices, books, and records, including policies and procedures relating to the security of Electronic PHI received from, created by or received by Business Associate on behalf of Covered Entity, available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's, Business Associate's compliance with the Security Rule.
- 3.8 Cooperation in Security Compliance. Business Associate shall fully cooperate in good faith to assist Covered Entity in complying with the requirements of the Security Rule.
- 3.9 Refraining from intimidation or retaliation. A Covered Entity or Business Associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any Individual or other person for-- (a) Filing of a complaint under 45 C.F.R. § 160.306; (b) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or (c) opposing any act or practice made unlawful, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

#### **4. USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

- 4.1 Use and Disclosure of PHI for Operations on Behalf of Covered Entity. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform Treatment, Payment or Health Care Operations for, or on behalf of, Covered Entity as specified in Service Agreements, provided that such use or disclosure would not violate the Privacy and Security Rule, if done by Covered Entity.
- 4.2 Other Uses of PHI. Except as otherwise limited in this Agreement, Business Associate may use PHI within its Workforce as required for Business Associate's proper management and administration, not to include Marketing or Commercial Use, or to carry out the legal responsibilities of the Business Associate.
- 4.3 Third Party Disclosure Confidentiality. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or, if permitted by law, this Agreement, and the Service Agreement, provided that, if Business Associate discloses

any PHI to a third party for such a purpose, Business Associate shall enter into a written agreement with such third party requiring the third party to: (a) maintain the confidentiality, integrity, and availability of PHI and not to use or further disclose such information except as required by law or for the purpose for which it was disclosed, and (b) notify Business Associate of any instances in which it becomes aware in which the confidentiality, integrity, and/or availability of the PHI is Breached immediately upon becoming aware.

4.4 Other Uses Strictly Limited. Nothing in this Agreement shall permit the Business Associate to share PHI with Business Associate's affiliates or contractors except for the purposes of the Service Agreement(s) between the Covered Entity and Business Associate(s) identified in the "LIST OF AGREEMENTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT" on page one (1) of this Agreement.

4.5 Covered Entity Authorization for Additional Uses. Any use of PHI or other confidential HCFA information by Business Associate, its Subcontractors, its affiliate or Contractor, other than those purposes of this Agreement, shall require express written authorization by the Covered Entity, and a Business Associate agreement or amendment as necessary.

Activities which are prohibited include, but not are not limited to, Marketing or the sharing for Commercial Use or any purpose construed by Covered Entity as Marketing or Commercial use of HCFA enrollee personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws.

4.6 Prohibition of Offshore Disclosure. Nothing in this Agreement shall permit the Business Associate to share, use or disclose PHI in any form via any medium with any third party beyond the boundaries and jurisdiction of the United States without express written authorization from the Covered Entity.

4.7 Prohibition of Other Uses and Disclosures. Business Associate shall not use or disclose PHI that is Genetic Information for underwriting purposes. Moreover, the sale, marketing or the sharing for commercial use or any purpose construed by Covered Entity as the sale, marketing or commercial use of HCFA enrollee personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws, is prohibited.

4.8 Data Use Agreement - Use and Disclosure of Limited Data Set. Business Associate may use and disclose a Limited Data Set that Business Associate creates for Research, public health activity, or Health Care Operations, provided that Business Associate complies with the obligations below. Business Associate may not make such use and disclosure of the Limited Data Set after any cancellation, termination, expiration, or other conclusion of this Agreement.

4.9 Limitation on Permitted Uses and Disclosures. Business Associate will limit the uses and disclosures it makes of the Limited Data Set to the following: Research, public health activity, or Health Care Operations, to the extent such activities are related to covered functions, including business planning and development such as conducting cost-management and planning-related analysis related to managing and operating Business Associates functions, formulary development and administration, development and improvement of methods of payment or coverage policies, customer service, including the provision of data analysis for policy holders, plan sponsors, or other customers, to the extent such activities are related to covered functions, provided that PHI is not disclosed and disclosure is not prohibited pursuant to any other provisions in this Agreement related to Marketing or Commercial use.

- 4.10 Business Associate shall enter into written agreements that are substantially similar to this Business Associate Agreements with any Subcontractor or agent which Business Associate provides access to Protected Health Information.
- 4.11 Business Associates shall implement and maintain information security policies that comply with the HIPAA Security Rule.

## 5. OBLIGATIONS OF COVERED ENTITY

- 5.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of Privacy Practices produced by Covered Entity in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice.
- 5.2 Notice of Changes in Individual's Access or PHI. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses.
- 5.3 Notice of Restriction in Individual's Access or PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use of PHI.
- 5.4 Reciprocity for Requests Received by Business Associate. The Parties agree that this Section (Section 5) is reciprocal to the extent Business Associate is notified or receives an inquiry from any Individual within Covered Entity's covered population.

## 6. TERM AND TERMINATION

- 6.1 Term. This Agreement shall be effective as of the date on which it has been signed by both parties and shall terminate when all PHI which has been provided, regardless of form, by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if the Parties agree that it is unfeasible to return or destroy PHI, subsection 6.3.5 below shall apply.
- 6.2 Termination for Cause. This Agreement authorizes and Business Associate acknowledges and agrees Covered Entity shall have the right to terminate this Agreement and Service Agreement in the event Business Associate fails to comply with, or violates a material provision of this Agreement and any provision of the Privacy and Security Rules.
- 6.2.1 Upon Covered Entity's knowledge of a Breach by Business Associate, Covered Entity shall either:
- a) Provide notice of breach and an opportunity for Business Associate to reasonably and promptly cure the breach or end the violation, and terminate this BAA if Business Associate does not cure the breach or end the violation within the reasonable time specified by Covered Entity; or
  - b) Immediately terminate this BAA if Business Associate has breached a material term of this BAA and cure is not possible.
- 6.3 Effect of Termination. Upon termination of this Agreement for any reason, except as provided in subsections 6.3.2 and 6.3.5 below, Business Associate shall at its own expense either return and/or destroy all PHI and other confidential information received

from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision applies to all confidential information regardless of form, including but not limited to electronic or paper format. This provision shall also apply to PHI and other confidential information in the possession of sub-contractors or agents of Business Associate.

- 6.3.1 The Business Associate shall consult with the Covered Entity as necessary to assure an appropriate means of return and/or destruction and shall notify the Covered Entity in writing when such destruction is complete. If information is to be returned, the Parties shall document when all information has been received by the Covered Entity.
- 6.3.2 This provision (Section 6.3 and its subsections) shall not prohibit the retention of a single separate, archived file of the PHI and other confidential HCFA information by the Business Associate if the method of such archiving reasonably protects the continued privacy and security of such information and the Business Associate obtains written approval at such time from the Covered Entity. Otherwise, neither the Business Associate nor its Subcontractors and agents shall retain copies of HCFA confidential information, including enrollee PHI, except as provided herein in subsection 6.3.5.
- 6.3.3 The Parties agree to anticipate the return and/or the destruction of PHI and other HCFA confidential information, and understand that removal of the confidential information from Business Associate's information system(s) and premises will be expected in almost all circumstances. The Business Associate shall notify the Covered Entity whether it intends to return and/or destroy the confidential with such additional detail as requested. In the event Business Associate determines that returning or destroying the PHI and other confidential information received by or created for the Covered Entity at the end or other termination of the Service Agreement is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction unfeasible.
- 6.3.4 Except for Business Associate Agreements in effect prior to April 21, 2005 when the Security Rule became effective, for the renewal or amendment of those same Agreements, or for other unavoidable circumstances, the Parties contemplate that PHI and other confidential information of the Covered Entity shall not be merged or aggregated with data from sources unrelated to that Agreement, or Business Associate's other business data, including for purposes of data backup and disaster recovery, until the parties identify the means of return or destruction of the HCFA data or other confidential information of the Covered Entity at the conclusion of the Service Agreement, or otherwise make an express alternate agreement consistent with the provisions of Section 6.3 and its subsections.
- 6.3.5 Upon written mutual agreement of the Parties that return or destruction of PHI is unfeasible and upon express agreement as to the means of continued protection of the data, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction unfeasible, for so long as Business Associate maintains such PHI.

## 7. MISCELLANEOUS

- 7.1 Regulatory Reference. A reference in this Agreement to a section in the Privacy and/or Security Rule means the section as in effect or as amended.
- 7.2 Amendment. The Parties agree to take such action to amend this Agreement from time to

time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191. Business Associate and Covered Entity shall comply with any amendment to the Privacy and Security Rules, the Health Insurance Portability and Accountability Act, Public Law 104-191, and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended, including, but not limited to, changes required by the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

- 7.3 Survival. The respective rights and obligations of Business Associate under Confidentiality and Section 6.3 of this Agreement shall survive the termination or expiration of this Agreement.
- 7.4 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the Privacy and Security Rules.
- 7.5 Headings. Paragraph Headings used in this Agreement are for the convenience of the Parties and shall have no legal meaning in the interpretation of the Agreement.
- 7.6 Notices and Communications. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by electronic mail, hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective party at the appropriate facsimile number or address as set forth below, or to such other party, facsimile number, or address as may be hereafter specified by written notice. (For purposes of this section, effective notice to "Respective Party" is not dependent on whether the person named below remains employed by such Party.) The Parties agree to use their best efforts to immediately notify the other Party of changes in address, telephone number, and fax numbers and to promptly supplement this Agreement as necessary with corrected information.

**Notifications relative to Sections 2.7, 3.4 and 3.5 of this Agreement must be reported to the Privacy Officer pursuant to Section 3.6.**

COVERED ENTITY:	BUSINESS ASSOCIATE:
Darin J. Gordon, Director	_____
Department of Finance and Adm.	_____
Health Care Finance & Admin.	_____
310 Great Circle Rd.	_____
Nashville, TN 37243	_____
Phone: (615) 507-6443	_____
Fax: (615) 253-5607	_____

All instructions, notices, consents, demands, or other communications shall be considered effectively given as of the date of hand delivery; as of the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing; or on the day the facsimile transmission is received mechanically by the facsimile machine at the receiving location and receipt is verbally confirmed by the sender.

- 7.7 Transmission of PHI or Other Confidential Information. Regardless of the transmittal methods permitted above, Covered Entity and Business Associate agree that all

deliverables set forth in this Agreement that are required to be in the form of data transfers shall be transmitted between Covered Entity and Business Associate via the data transfer method specified in advance by Covered Entity. This may include, but shall not be limited to, transfer through Covered Entity's SFTP system. Failure by the Business Associate to transmit such deliverables in the manner specified by Covered Entity, may, at the option of the Covered Entity, result in liquidated damages as set forth in one (1) or more of the Service Agreements between Covered Entity and Business Associate listed above. All such deliverables shall be considered effectively submitted upon receipt or recipient confirmation as may be required.

- 7.8 **Strict Compliance.** No failure by any Party to insist upon strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement.
- 7.9 **Severability.** With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.
- 7.10 **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that Tennessee law has been pre-empted by HIPAA and HITECH and without giving effect to principles of conflicts of law. Jurisdiction shall be Davidson County, Nashville, Tennessee, for purposes of any litigation resulting from disagreements of the parties for purpose of this Agreement and the Service Agreement (s).
- 7.11 **Compensation.** There shall be no remuneration for performance under this Agreement except as specifically provided by, in, and through, existing administrative requirements of Tennessee State government and Services Agreement(s) referenced herein.
- 7.12 **Validity of Execution.** Unless otherwise agreed, the parties may conduct the execution of this Business Associate Agreement transaction by electronic means. The parties may agree that an electronic record of the Agreement containing an Electronic Signature is valid as an executed Agreement.

IN WITNESS WHEREOF, the Parties execute this Agreement to be valid and enforceable from the last date set out below:

**HEALTH CARE FINANCE & ADMINISTRATION**

**BUSINESS ASSOCIATE**

By: \_\_\_\_\_  
**Darin Gordon, Director**  
 Date: \_\_\_\_\_  
 State of Tennessee, Dept. of Finance & Adm.  
 310 Great Circle Road Nashville, TN 37243  
 Phone: (615) 507-6443 Fax: (615) 253-5607

By: \_\_\_\_\_  
 \_\_\_\_\_  
 Date: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

---

## DATA SOURCES INFORMATION

### 5.1 Data Sources

- 5.1.1 The migration of legacy State Eligibility data includes, but is not be limited to, the data sources listed below:
- 5.1.1.1 MMIS (InterChange) - MMIS Interchange database that contains Medicaid Member case and claims information for Members that are currently enrolled in Medicaid for the State of Tennessee. It also contains historic case and claims information for past Members that are no longer enrolled. There are currently more than 1.5 million active Medicaid Members in InterChange. While InterChange is not an Eligibility Determination System and does not contain data concerning the factors that are used to determine Eligibility, it does serve as the authoritative source of which Members are currently eligible and active Medicaid beneficiaries.
  - 5.1.1.2 Automated Client Certification and Eligibility Network for Tennessee (ACCENT) – Mainframe IMS/DB2
  - 5.1.1.3 CoverKids/CHIP Data – AHS vendor data (approximately 75,000 enrollees)
  - 5.1.1.4 Beneficiary and Earning Data Exchange - Provides Medicare entitlement and earning information for Medicaid Members
  - 5.1.1.5 Customer Relationship Management – TNHC Data
  - 5.1.1.6 SSA - The SSA State Data Exchange (SDX) provides detailed information about Medicaid Members receiving social security benefits

---

## **ADDITIONAL SDLC AND OPERATIONS AND MAINTENANCE INFORMATION**

### **5.1 Introduction**

- 5.1.1 The Information Technology capabilities outlined below are the foundation for what the Contractor shall be required to deliver throughout the System Development Lifecycle (SDLC) of the program. These requirements are the source for which the Contractor shall base their strategy, approach, and staffing plans on for the design, development, and implementation (DDI) and Maintenance O&M of the system.

### **5.2 Stakeholder Analysis & Management**

- 5.2.1 Stakeholder Management and Analysis is used to identify the project's key stakeholders and their roles and responsibilities within the project, provide an analysis of their interests in and attitude towards the effort, and manage stakeholder participation to secure positive support for the project. The Stakeholder Analysis and Management capability identifies the impacted groups or individuals and their needed level of commitment and establishes detailed engagement plans for impacted stakeholders to ensure project success. The Stakeholder Analysis and Management Plan will define the approach to identifying, analyzing, recording, and maintaining the stakeholders for each Program project in a Program Stakeholder Register.
- 5.2.2 Achieving insight early enables active Stakeholder Management to achieve sustainable commitment, using a range of interventions to explore barriers, build commitment and trust, leverage stakeholders' organizational influence, and establish change agent networks, as needed.

### **5.3 Business Analysis Management**

- 5.3.1 Business Analysis Management is the practice of reviewing business processes or solutions and determining the business needs in relation to such process or Solution. The Business Analyst is the practitioner tasked with performing business analysis, and serves as the liaison between the business owners, solution development teams and testing teams. The Business Analyst fills the role as an advocate for the correct interpretation and application of requirements through the Solution lifecycle and providing oversight to the accuracy and completeness of the Requirements Traceability Matrix. As part of reviewing processes and solutions, the Business Analyst will take a holistic view of the process or Solution, identify areas for improvement, and document the requirements needed for improving such process or Solution.

### **5.4 Business Process Management**

- 5.4.1 BPM is a systematic approach to controlling the business processes in an organization, with the goal of making the organization's workflow more effective, more efficient and more capable of adapting to changes and opportunities in the environment. BPM may involve any combination of modelling, automation, execution, control, measurement and optimization of business activity flows, in support of enterprise goals, spanning systems, employees, customers and partners within and beyond the enterprise boundaries. It includes activities to assess, change, and monitor business processes to support improved organizational performance and service delivery quality and efficiency.

## **5.5 Business Rules Management**

- 5.5.1 Business Rules Management is the discipline that includes processes and standards for identifying, analyzing, documenting, and managing business rules, which are constraints, conditions, or directives used to determine an appropriate business action.

## **5.6 Requirements Management**

- 5.6.1 Requirements Management is the process of collecting, analyzing, refining, and prioritizing Solution requirements and planning for their delivery. By tracking Solution requirements from identification of the business need through deployment of the associated functionality, requirements management helps to ensure that customer and stakeholder needs are defined, documented, and addressed through the Solution lifecycle.

## **5.7 Test Management**

- 5.7.1 The Test Management capability validates that the Solution has met the business requirements as well as the technical design specifications. Testing must be comprehensive of all elements of the Solution, including development, integration, security, performance and accessibility. Effective testing must include documentation for test case execution, pass/fail determination for expected results, as well as screen print verification of test execution and result determination cross referenced to the requirement traceability matrix.

## **5.8 Interface/Integration Management**

- 5.8.1 Interface and Integration Management addresses the need for information sharing across systems and organizations. Given the criticality of information from multiple sources as part of the eligibility determination, the Contractor shall be responsible for developing, executing, managing and maintaining a secure and highly available Interface and Integration Management Plan that aligns with State and Federal regulations and standards, industry standards and the CMS Seven Conditions and Standards.

## **5.9 Integrated System Implementation Management**

- 5.9.1 Integrated System Implementation Management occurs prior to and during implementation activities to ensure a successful transition from the State's Eligibility as-is state, to its to-be state. Depending on the rollout approach, the complexity may vary but it is essential that the Contractor has a Management Plan in place for a seamless transition. Integrated System Implementation Management will impact business, technical, governance and project management stakeholders.

## **5.10 Post Implementation Evaluation**

- 5.10.1 Post Implementation Evaluation involves assessing the effectiveness of a specified Solution deployment with respect to the original goals of the business, helping to identify future Solution opportunities. A Post Implementation Review should be performed at a predetermined time post go-live, and shall include participation from all stakeholders relevant to the project.
- 5.10.2 Post implementation evaluation activities have the ability to realign current Solution and business needs, and strategically prioritize them with respect to the current production environment. The evaluation will assist the State in determining whether the Solution deployment met project and State expectations in terms of functionality, operational performance, costs vs. benefits realization, and system development life-cycle effectiveness.

### **5.11 Continuous Improvement Process (CIP)**

- 5.11.1 Continuous improvement process focuses on increasing the efficiency, maximizing the effectiveness and optimizing the performance of TEDS related services and the supporting IT service management processes. A mature, reliable and consistent CIP ensures that improvement opportunities are identified and addressed throughout the entire lifecycle of each service.
- 5.11.2 The primary purpose of the CIP is to continually align and re-align IT services to the State's changing needs by identifying and implementing improvements to IT services that support TEDS processes.

### **5.12 Service Level Management**

- 5.12.1 Service level management ensures that an agreed level of IT service is provided for all current IT services, and that future services are delivered to agreed achievable targets.

### **5.13 Service Portfolio and Service Catalogue Management**

- 5.13.1 The purpose of a service portfolio is to manage and describe the portfolio IT services in terms of business value and articulated business needs. The service catalogue is a key component of the service portfolio, which functions as the single source of accurate and consistent information regarding IT services. It also validates that this information is widely available to those who are authorized to access it.

### **5.14 Technology Capacity and Performance Management**

- 5.14.1 Technology capacity and performance management is the discipline of provisioning organizational IT resources (e.g., infrastructure storage) and services relative to business demands, to achieve satisfactory service levels in a cost efficient and timely manner. The objective of this capability is to have zero capacity and performance related incidents.

### **5.15 Availability Management**

- 5.15.1 Availability management is the discipline of ensuring that the services delivered are highly-reliable and highly available, as well as matching to or exceeding the current and future agreed needs of the business, in a cost-effective manner.

### **5.16 Business Continuity/Disaster Recovery (BC/DR)**

- 5.16.1 BC/DR is the discipline that ensures that the organization can resume its business and IT operations efficiently and effectively in the event of disaster. IT Service Continuity Management rationalizes the businesses capability and maturity, and provides the organization a rigorous process-oriented approach towards Business Continuity. The purpose is to design, develop, and implement IT Service Continuity Management; both as an organizational capability and as a strategic asset.

### **5.17 Service Transition Planning and Support**

- 5.17.1 Service transition planning and support focuses on coordinating the activities and resources required to efficiently move new services into production. In order for new services to be moved into production in an effective manner, all personnel and technical resources/constraints must be considered.

## **5.18 Technology Change Management**

- 5.18.1 Technology Change Management will ensure that IT releases and changes related to a product or system are introduced in a controlled and coordinated manner. It ensures the proper controls are in place to limit disruption to the production environment. The change/release management capability shall include well defined processes for continuous improvement.

## **5.19 Configuration Management**

- 5.19.1 Configuration management defines and controls the components of services and infrastructure, and maintains accurate configuration information on the historical, planned and current state of the services and infrastructure.

## **5.20 Release and Deployment Management**

- 5.20.1 Release and deployment management controls the plan with the approval of the Project Steering Committee, schedule, build, test, and ultimately controls the movement of releases into test and production environments. Movement of a release into the State's UAT environment and production environment requires approval of the State's Technical Change Control Board. Release and deployment management also ensures that the integrity of the production environment is protected and that the correct components are released.

## **5.21 Asset Management**

- 5.21.1 Asset management Identifies, classifies and tracks all software and hardware assets throughout their lifecycle from acquisition through disposal; includes licensing.

## **5.22 Event Management**

- 5.22.1 Event management consists of the detection, diagnosis, and determination of corrective action for events (A change of state that has significance for the management of an IT service or other configuration item (CI)).

## **5.23 Incident Management**

- 5.23.1 Incident management consists of the processes to detect, diagnose, and determine the corrective action for incidents (An unplanned interruption to an IT service or reduction in the quality of an IT service).

## **5.24 Problem Management**

- 5.24.1 Problem management is the process responsible for managing the lifecycle of all problems (the cause of one or more incidents). Problem management proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented.

## **5.25 Request Management**

- 5.25.1 Request management is the process for handling the lifecycle of service requests from users.

## **5.26 Technology Operations**

- 5.26.1 Technology operations is the discipline of designing, testing, operating and improving technology operations, as well as in developing the skills required to operate the IT infrastructure.