**RFP# 19-096 SCOPE OF WORK**

**ATTACHMENT C**

# **Introduction**

In accordance with Indiana statute, including IC 5-22-9, the Indiana Department of Administration (IDOA), acting on behalf of the Indiana Family and Social Services Administration (FSSA) Division of Family Resources (DFR) (<https://www.in.gov/fssa/2407.htm>), requests Maintenance and Operations (M&O) of the of the Application Services (AS) solution as well as Design, Development, and Implementation (DDI) of new or updated components to the AS solution. The AS solution provides Eligibility & Enrollment (E&E) online benefits, worker, and agency portal systems; Document Center systems; and Indiana Manpower and Comprehensive Training (IMPACT) support needs for DFR.

The Contractor awarded a contract via this RFP will be expected to maintain these AS solution components and provide enhancements that comply with all aspects of:

* Centers for Medicare & Medicaid Services (CMS) applicable requirements (<https://www.medicaid.gov/medicaid/data-and-systems/meet/index.html>) for Health Coverage E&E,
* United State Department of Agriculture (USDA) Food and Nutrition Service (FNS) applicable requirements (<https://www.fns.usda.gov/apd/fns-handbook-901-v2-advance-planning-documents>) for Supplemental Nutrition Assistance Program (SNAP) and Employment & Training (E&T) (<https://www.fns.usda.gov/snap/et-state-plan-handbook>, and
* Administration for Children & Families (ACF) applicable requirements for Temporary Assistance for Needy Families (TANF) and Employment & Training (E&T).

# **Background and Purpose**

* 1. **Application Services Overview**

AS is overseen by DFR. All AS solution components are currently hosted by the Indiana Office of Technology (IOT). All AS solution components (both in production and non-production environments) developed or maintained as part of this Contract scope shall be hosted by IOT throughout the term of the resulting contract from this RFP.

AS solution components were implemented from 2007 through 2012, with the IMPACT solution replacing another E&T system in 2017. These solution components were introduced to support standardization and improved operational processes for DFR, while also giving clients access to an electronic portal and improved document processing. Throughout the years, AS solution components have improved and evolved significantly to accommodate client and worker needs as well as Federal and State requirements for business, policy, information technology (IT), security, and privacy expectations.

**DFR has adopted microservice architecture with container virtualization for new AS components. This modern approach adopted by the SDLC industry at large and DFR itself has increased responsiveness to client, operational, and policy needs. The SDLC can generate updates more quickly for the business while maintaining patching, upgrades, and other maintenance-oriented support. It is expected that the Contractor will maintain this modern architecture while also providing additional architecture and infrastructure solutions with modern approaches throughout the term of this agreement to continually improve DFR systems. In delivering these modern approaches in alignment with State, CMS MITA, and FNS objectives, DFR is further expecting that solutions will be easily and cost effectively supportable and replaceable when components must be upgraded or substituted.**

The AS solution is comprised of the following components that have interrelationships due to interfaces or shared platforms:

|  |  |  |
| --- | --- | --- |
| **AS Solution Component** | **Description** | **Major Technology and Architecture** |
| **Benefits Portal** | * <https://fssabenefits.in.gov/> * Provides functionality for clients and Authorized Representatives to apply for Health Coverage, SNAP, and/or Cash Assistance (TANF) * Screening tool for clients to determine “Am I Eligible” for benefits without committing to application * Provides functionality to clients for determining current case status, printing proof of eligibility, reporting changes, and having access to other helpful information | * Based on Java frameworks and non-relational document-oriented (MongoDB) |
| **Agency Portal** | * <https://www.fssabenefits.in.gov/AgencyPortal/#/> * Provides functionality for authorized agencies working with clients receiving public assistance through DFR E&E to determine case status for clients who approve this access (e.g., Area Agencies for Aging, navigators) * Additional details: <https://www.in.gov/fssa/dfr/4323.htm> | * Java frameworks * Oracle 12c |
| **IMPACT Worker Portal** | * Intranet URL * Used by DFR and E&T vendor staff for supporting the IMPACT program * Additional details: <https://www.in.gov/fssa/dfr/2682.htm> | * Java frameworks * Oracle 12c |
| **Document Center** | * Intranet URLs * Template-based document system augmented by barcoding strategy for document types. This strategy allows documents coming into Document Center operations to be indexed directly to cases while supporting standardized processes for Document Center workers and E&E staff * To be updated with new Content Manager platform and upgrade/replacement of Captiva (see Section 7.10) | * Captiva * IBM Content Manager * Oracle 12c |
| **I3/Interactive Voice Response (IVR)** | * Intranet URLs and phone/fax number for external callers   + Fax number for routing documents to Document Center * Mature IVR with call routing to role-based workers/management via queues * Reporting of call data * Average of 20,600 calls received monthly over the first half of 2018. Calls can increase greatly when new functionality or enhancement rolls out | * Genesys PureConnect I3 on premise solution * Java frameworks / .NET * DB2 |
| **Communication & Document Management System (CDMS)** | * Document Processing System (DPS)   + Intranet URL | * Java frameworks * Oracle 12c |
| * Call Center System (CCS)   + Intranet URL |
| * Electronic Message System (eMS)   + Intranet URL |
| **Based on Legacy Cúram Technology (the components below to be replaced by IEDSS and decommissioned by legacy Contractor)** | | |
| **Worker Portal** | * Intranet URL * To be replaced by the Indiana Eligibility Determination and Services System (IEDSS) solution’s Worker Portal * Part of Family Assistance & Care through Technology Service (FACTS) * Used by DFR E&E workers for access to client documents and task management that drives the DFR E&E business model * Allows access to E&E documents indexed to cases via Document Center solution * Adobe LiveCycle exists in this solution but will be decommissioned with the conclusion of the IEDSS rollout | * IBM Cúram 5.2 * Legacy Java frameworks * IBM DB2 |
| **Hearings & Appeals Worker Portal** | * Intranet URL * To be replaced by IEDSS solution’s Worker Portal * Used by FSSA Office of Hearings and Appeals (OHA) workers and other support staff for facilitating Hearings & Appeals processes for clients | * IBM Cúram * Legacy Java frameworks * IBM DB2 |

AS is managed and support by one (1) incumbent vendor. When the contract that results from this RFP begins on January 1, 2020, the two (2) month transition period will begin for the Contractor to prepare for taking over M&O responsibilities from the incumbent vendor on March 1, 2020. The Contractor’s M&O responsibilities will cover the following six (6) AS solution components:

1. Benefits Portal M&O
2. Agency Portal M&O
3. CDMS M&O
4. Document Center M&O
5. IMPACT M&O
6. I3/IVR M&O

**The M&O for the legacy Cúram-based Worker Portal and the legacy Cúram-based Hearings & Appeals Module are not in scope for this RFP.** The M&O for these two components will continue to be provided by the incumbent AS vendor until they are replaced by the IEDSS Worker Portal (rollout anticipated to complete by end of 2019). The incumbent AS vendor will support decommissioning of these legacy components in no more than six (6) months. From January 1-February 29, 2020, the incumbent AS vendor will be available to help transition the M&O responsibilities for the six (6) in-scope AS components to the Contractor. Starting March 1, 2020, the incumbent AS vendor may be available for up to four (4) months to address remaining questions about any M&O components.

While there are several solution components to be maintained and/or enhanced, the incumbent vendor has individual staff dedicated to multiple maintenance and enhancement efforts. The Contractor will be expected to provide this same staffing strategy for supporting the scope described in this RFP. Today, AS is being supported by approximately 80 FTEs. This is broken down to approximately 24% testers, 16% Java developers, 15% administrative staff, 11% operations staff, 10% business analysts, 5% Captiva developers, 6% Cúram developers, 4% database administrators, 3% interface developers, 3% I3/IVR developers, and 3% reporting business analysts/developers. This quantity, with some growth to this count but with minimal variance, has been provided over the years by the incumbent. It is not anticipated that the Contractor would provide this exact FTE count as the State is receptive to evaluation of a different staffing model than the incumbent vendor’s mix. Additionally, the Contractor will not need to provide Cúram developers as the incumbent AS vendor will retain M&O responsibilities for the two legacy Cúram-based components.

* 1. **AS Major Interface Partners**

The AS solution components’ most significant interface partners (see Section 2.4 for all partners) are:

* The Indiana Client Eligibility System (ICES) solution is the current system of record for E&E. This system will be replaced by the IEDSS solution.
* The Staff Management and Resource Tracking (SMART) system organizes worker tasks from the FACTS and ICES solutions for E&E operations while also providing Quality Assurance (QA) support. This system will be replaced by the IEDSS solution.
* The Indiana Eligibility Determination Services System (IEDSS): The IEDSS Worker Portal will be replacing the Eligibility Worker Portal, the OHA Portal, ICES, and SMART. It will be in production for the State starting late Spring 2019 and completed by early 2020 (the legacy system will be available in parallel with the new IEDSS Worker Portal until rollout is completed). The Contractor will be expected to support interfaces with IEDSS (note: the incumbent Contractor will support the legacy Eligibility Worker Portal and OHA Portal through decommission).
  1. **Organizational Overview and State/Federal Requirements**
     1. **State Entities and their Requirements for the AS Solution**

Below is additional background information about the State entities involved with the E&E solution components that AS provide.

1. **Family & Social Services Administration (FSSA)** – This agency supports Indiana healthcare and provides, administers, and funds social services. The six care divisions in FSSA administer to over one million Hoosiers. Please see the following site for more information: <https://www.in.gov/fssa/index.htm>. While the AS solution may have interfaces with several organizations within FSSA, for the purposes of this RFP, the entities within FSSA most applicable to AS are listed below (DFR, OMPP, and DST).
   1. AS must comply with all aspects of FSSA Security Policies: <https://www.in.gov/fssa/4979.htm>
2. **Division of Family Resources (DFR)** – This agency is the primary sponsor of AS and owner of all AS solution components. This agency is also held responsible by CMS, FNS, and ACF for complying with Federal E&E and E&T requirements. DFR: (1) establishes eligibility for Medicaid and Health Coverage, Supplemental Nutrition Assistance Program (SNAP), and Temporary Assistance for Needy Families (TANF) benefits; (2) manages the timely and accurate delivery of SNAP and TANF benefits with timely referral of Health Coverage recipient data to enrollment process and operations (see OMPP below), (3) provides employment and training services to IMPACT clients, and (4) focuses on the support and preservation of families by emphasizing self-sufficiency and personal responsibility.

Systems that DFR own are the following: Indiana Client Eligibility System (ICES), Family Assistance and Care through Technology Services (FACTS), Indiana Eligibility Determination Services System (IEDSS), Medical Review Team (MRT – used for Medicaid Aged, Blind, and Disabled support and interfaces with FACTS for tasking and documents as well as ICES/IEDSS), Staff Management and Resource Tracking (SMART), and IMPACT. DFR manages policy and system Subject Matter Experts (SMEs) with whom the Contractor will be expected to work with on all aspects of the Systems Development Life Cycle (SDLC) process, including garnering sign-off on requirements and design artifacts as well as overseeing go-live to production of AS solution components, based on UAT results (UAT will be conducted by DFR and their designees).

1. **Office of Medicaid Policy and Planning (OMPP)** – Administers Medicaid programs and performs medical review of Medicaid disability claims. OMPP’s suite of programs, called the Indiana Health Coverage Programs (IHCP), includes traditional Medicaid, risk-based managed care, Healthy Indiana Plan (HIP) 2.0, a variety of waiver services, and a prescription drug program tailored to the needs of specific populations. OMPP systems support enrollment and claims payment for the Health Coverage recipients deemed eligible by DFR systems. Systems that OMPP owns include the following: CORE MMIS, Pharmacy, and Management and Administrative Reporting (MAR).
2. **Division of Healthcare Strategies & Technologies (DST)** - Supports FSSA technology solutions and systems by providing technical managers, business/system analysts, database administrators (DBAs), security and privacy staff, and developers to FSSA divisions and processes. The Contractor will be expected to work throughout the SDLC process with DST technical and system business analysts.
3. **Indiana Office of Technology (IOT)** - Provides measurable, secure, consistent, reliable enterprise technology services at cost-effective prices to partner agencies so they can better serve the mutual customer, the Hoosier taxpayer. All AS M&O and DDI scope is anticipated to have production and non-production solution components hosted by IOT throughout the term of the resulting contract from this RFP. While DFR and the Contractor may work with several entities within IOT to support AS operations, a dedicated team within IOT currently reports to DFR and supports all aspects of AS infrastructure (as well as other DFR systems). IOT is also a sponsor of production AS solution releases, so the Contractor will be expected to interact with IOT throughout all aspects of the SDLC process.
   1. The Contractor and the AS solution must comply with all aspects of IOT Policies, Procedures, and Standards, including the Information Security Framework:
      1. IOT Policies, Procedures, and Standards: <https://www.in.gov/iot/2394.htm>
      2. IOT Information Security Framework: <https://www.in.gov/iot/files/Information_Security_Framework.pdf>
      3. IOT Project Review Policy: <https://www.in.gov/iot/files/project_review_policy_20110311_final.docx>
      4. **Federal Agencies, Programs, and their Requirements for the AS Solution**

**Centers for Medicare & Medicaid Services (CMS)**

CMS supports the Medicaid program, which is funded by Federal and State sources. State of Indiana FSSA Healthcare Assistance programs (funded by the Medicaid program) support the medical care of persons who meet specific categorical non-financial, income, and resource requirements. Individuals can be eligible for full, limited, or emergency Medicaid coverage depending on the category under which they qualify.

Also funded by CMS, the Children’s Health Insurance Program (CHIP) provides comprehensive coverage, with some limitations, for eligible children under the age of 19 who pay a premium based on family income.

Hoosier Healthwise for Children, Families, and Pregnant Women blends Medicaid and CHIP seamlessly for applicants and members while efficiently achieving the Federal requirement to screen all children first for Medicaid before enrolling them in CHIP.

Healthy Indiana Plan (HIP) 2.0 is a Medicaid demonstration waiver under Section 1115(a) of the Social Security Act. The design of the HIP 2.0 program was set forth in compliance with the Patient Protection and Affordable Care Act (PPACA).

While Presumptive Eligibility in Indiana is available under PPACA requirements, Presumptive Eligibility for Pregnant Women specifically supports ambulatory pre-natal care to pregnant women who are determined eligible by a qualified provider, while their Medicaid application is pending.

In terms of E&E system requirements, CMS has set forth expectations that are applicable to AS solution components and processes. The Contractor will be expected to support FSSA’s compliance with these expectations. In reviewing the requirements below, note that they are heavily interrelated and reference each other (e.g., the Medicaid Eligibility and Enrollment Toolkit (MEET) references MARS-E 2.0, MITA, and Standard and Conditions for Medicaid):

* MEET
  + See more information at this link: <https://www.medicaid.gov/medicaid/data-and-systems/meet/index.html>
  + AS must support the State in complying with the requirements listed in MEET checklists as well as all other expectations noted. Several of the checklist items will be mandatory (e.g., streamlined application requirements)
* The Conditions & Standards along with Expanded Conditions for E&E systems and Medicaid Management Information Systems (MMISs):
  + 42 CFR 433.112(b)(12) that was revised in 2016
    - See more information at this link: <https://www.medicaid.gov/federal-policy-guidance/downloads/smd16009.pdf>
  + Currently, the State complies with all aspects of these Conditions & Standards, and the Contractor is expected to support ongoing compliance.
* Medicaid Information Technology Architecture (MITA) 3.0: See more information at this link: <https://www.medicaid.gov/medicaid/data-and-systems/mita/index.html>
  + Currently, the State complies with MITA 3.0 expectations, and the Contractor is expected to support ongoing compliance with MITA 3.0 and maturity improvements, where applicable. Current MITA status details will be shared with the Contractor at the beginning of the contract term.
* Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0: See more information at this link: <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2-MARS-E-v2-0-Minimum-Acceptable-Risk-Standards-for-Exchanges-11102015.pdf>
  + The Contractor and AS is required to track ongoing compliance with all controls and expectations as dictated by MARS-E 2.0. Upon contract commencement, the Contractor will be provided access to the artifacts that have been maintained so far for AS by the current Contractor and the State (i.e., System Security Plan (SSP) and Plan of Action & Milestones (POA&M)).
* 42 CFR 433.112 (b)(5) and (6), and 45 CFR 95.617(a))

**United States Department of Agriculture (USDA) Food and Nutrition Service (FNS)**

FNS supports the Supplemental Nutrition Assistance Program (SNAP) as well as Employment & Training (E&T) programs.

The purpose of the SNAP Program is to assist eligible low-income participants to obtain a more nutritious diet by increasing food purchasing power. The purpose of E&T programs is to encourage and support applicable members of the SNAP household in gaining skills, training, work, and/or experience that will increase their ability to obtain regular, effective employment. FNS is responsible for establishing the regulations and providing states with direction in policy, management, funding, operations, and systems.

For E&T, the State has created the IMPACT program, which is in alignment with FNS and ACF E&T Program requirements (see below for FNS and additional details on IMPACT). IMPACT also refers to the case management tool for assigning, scheduling, and tracking employment activities while supporting the issuance of supportive services to IMPACT participants.

In terms of E&E and E&T system requirements, FNS has set forth expectations that are applicable to AS solution components and processes. The Contractor will be expected to support DFR’s compliance with these expectations:

* FNS Handbook 901: <https://www.fns.usda.gov/apd/fns-handbook-901-v2-advance-planning-documents>
* FNS E&T State Plan Handbook: <https://www.fns.usda.gov/snap/et-state-plan-handbook>
* SNAP Review of Major Change in Program Design and Management Evaluation Systems: <https://www.fns.usda.gov/snap/fr-011916>
  + These requirements apply to major enhancements stemming from Change Management and DDI components of this RFP
* FNS Test Plan requirements: <https://www.fns.usda.gov/apd/new-rule-system-testing>

**Administration for Children & Families (ACF)**

The Temporary Assistance for Needy Families (TANF) and Refugee Cash Assistance (RCA) programs are supported by ACF. These programs are designed to provide financial assistance to individuals who meet specific program eligibility requirements helping them gain self-sufficiency.

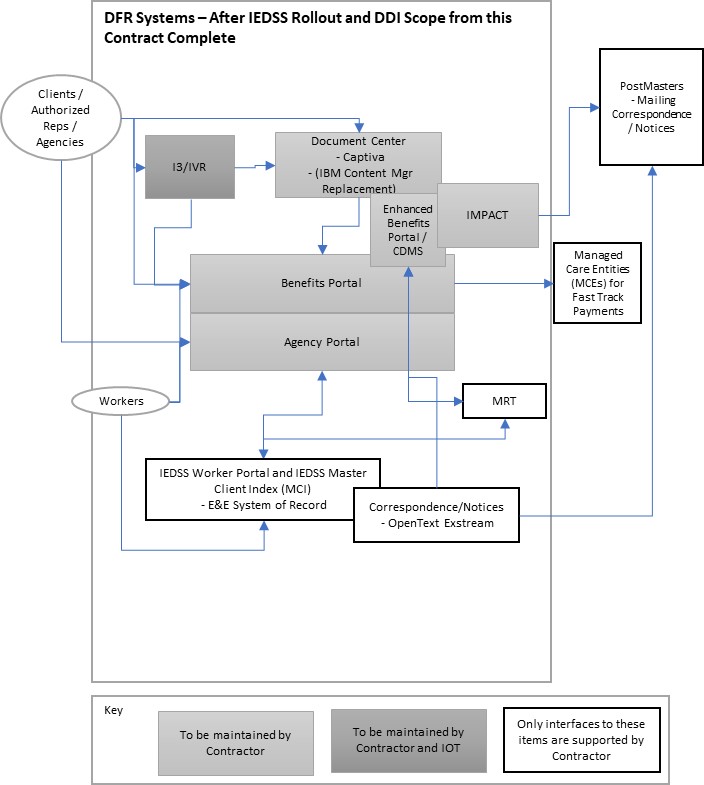
For additional details on ACF and their role in E&E and E&T, visit <https://www.acf.hhs.gov/>.

* + 1. **Other Standards**

In addition to the Federal and State requirements noted above, the Contractor shall comply with:

* SDLC best practices for effective IT solution delivery: Waterfall, Agile, Kanban, Scrum, and/or other related best practices may be considered (see <http://www.in.gov/iot/2394.htm> for more information)
* The Open Web Application Security Project (OWASP)
* Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794 (d))
  + Note that this is described also in the CMS MEET and in FNS requirements
* See Attachment B Section 12 for additional details on security and privacy regulations and requirements
  1. **AS Solution Design: Current and Future**

The diagram below represents the current high-level components of the AS solution.

****

* “DFR Systems – After IEDSS Rollout”: This box represents all of the components that are hosted on the State network supported by IOT. The dark grey boxes are to be maintained by the Contractor, with IOT supporting the infrastructure
* “Clients / Authorized Reps / Agencies”: These users of AS systems interact via phone, online, and with paper or fax submissions. While most are outside of the State network, some users are supported by the State network in State agencies outside of FSSA
* “Workers”: These users of eligibility systems interact via phone, online, and with paper submissions. While most are supported on the State network, some may access remotely (i.e., outside the State network)
* “IEDSS Worker Portal and IEDSS Master Client Index (MCI)”: These components are the eligibility system of record and MCI of all DFR clients. These critical components have interfaces with AS components to provide workers access to eligibility documents. Further, these interfaces support Clients/ARs/Agencies in providing eligibility information to the Benefits Portal and Agency Portal. Many other eligibility-related interfaces are pertinent to IEDSS but are not depicted on this diagram since they are not applicable to AS. IEDSS infrastructure is supported by IOT on the State network
  + “Correspondence/Notices – OpenText Exstream”: This component supports the IEDSS solution and workers in generating eligibility correspondence and notices. These resulting mailings are distributed via the PostMasters vendor and system solution (batch interfaces). These mailings are then made available for future client/AR/provider and worker access in the Document Center and CDMS system components
* “Medical Review Team (MRT)”: This eligibility system and unit of workers support Medicaid Aged, Blind, and Disabled (MA ABD) determinations. This work effort requires applicable MA ABD documentation and processing conducted in alignment with the IEDSS solution. MRT infrastructure is supported by IOT on the State network
* “Managed Care Entities (MCEs) for Fast Track Payments”: Fast Track Eligibility Credit Card Payments are supported via interfaces to MCEs in Indiana. When applicants apply for Health Coverage, in the event that they are eligible for HIP 2.0 and Fast Track Eligible, their credit card payment can be collected for immediate Power Account (PAC) payment in support of HIP 2.0 coverage. Except for applicable interface architecture, MCE infrastructure is not supported on the State network
* “PostMasters – Mailing Correspondence / Notices”: This vendor and system solution provides eligibility mailing support for the IMPACT and IEDSS system components (batch interfaces). These mailings are then made available for future client/AR/provider and worker access in the Document Center and CDMS system components. Except for applicable interface architecture, PostMasters infrastructure is not supported on the State network
  1. **AS Solution Users**

The following table contains the estimated count of end users per solution component. Note that there is some overlap in users across the various components as a single user may have access to multiple components. The numbers noted below are based only on the quantities of users who directly use the components noted.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User Type** | **Benefits Portal** | **Agency Portal** | **IMPACT Worker Portal** | **Document Center /CDMS** | **I3/IVR** |
| **Clients / Authorized Representatives (ARs) (Clients include applicants and current benefit recipients. ARs are those who represent clients in eligibility processes, upon agreement between the client and the AR.)** | 2 million or more total (This amount is the total quantity with which DFR interacts throughout the year. Around 75% may interact with the online portal while others rely on I3/IVR and paper processes. 1.5 million of these are current benefit recipients.) | 0 (They attest to particular agencies accessing their data, but they do not use it directly.) | 0 (Caseworker for clients is done in the IMPACT system but they do not directly interact.) | 0 (Client/ARs submit mail to the Document Center but do not use any of these systems directly.) | See “Benefits Portal” |
| **Agencies (non-DFR agencies who work with clients and/or ARs)** | See above (Some agency representatives may be ARs – see above.) | Approximately 500 agencies with approved access (~5 users per agency). | 0 | 0 | N/A |
| **E&E Workers** | 0 | 0 (Contractor operates this Portal) | 250 | 3,500 | 3,500 |
| **OHA Workers** | 0 | 0 | 0 | 0 | 50 |
| **IMPACT staff** | 0 | 0 | 250 | 0 | 250 |
| **Agency Portal Admin staff (Contractor to provide this support)** | 0 | 2 | 0 | 0 | 0 |
| **Benefits Portal Admin staff (Helpdesk vendor)** | ~10 | 0 | 0 | 0 | 0 |

As mentioned in Section 2.1, there is an average of 20,600 calls received monthly based on review of call data for the first half of 2018. However, calls can increase greatly for a period of time following the rollout of new functionality or enhancements.

* 1. **AS Solution Technologies and Tools**

The State mandates the use of State-approved technologies for the AS solution. The high-level technologies and tools are shown in the table below, and this information is not considered to be an exhaustive listing. For each system, the technologies/tools are listed for the server/infrastructure, the workstations that the Contractor will use to provide support, and what end users (Section 2.5) should have available to them. The following information for each technology/tool within a system are included: the version, a brief description, and general information regarding the Contractor versus State responsibilities.

**The use of new, modern approaches and technologies that are cost effective, secure, and supportive for clients and workers is encouraged, in alignment with State, CMS MITA, and FNS objectives.** However, any new technology or changes to the listing below is subject to the Change Management process (see Section 7.2).

Note that the listing below is considered high level and not exhaustive, with only the major components of each system noted. Other unlisted open source software, development libraries, and associated tools exist as parts of, or as supplements to, the tools listed. Versions that are listed may be subject to change during the time period from RFP issuance to the start of the Contract Term, depending upon the timing of patching or upgrades. Detailed listings of all servers, all installations on these servers, including baseline configuration details of all components, will be provided to the Contractor at the beginning of the Contract. See Attachment J for technical diagrams associated with each of the AS solution components.

Unless otherwise noted, server hardware and software licensure (production and non-production) for AS solutions will be provided by the State. Workstation and Contractor location hardware, software, and network licensure is the responsibility of the Contractor, unless otherwise noted.

**Assume production and non-production environments sufficient to support the SDLC are required for all of the technologies/tools listed.**

**Server Tools / Technologies:**

| **Server Software** | **Tool / Technology** | **Version** | **Brief Description of the Purpose** | **Contractor Responsibility** | **State Responsibility** |
| --- | --- | --- | --- | --- | --- |
| **Agency Portal** | | | | | |
| Java | IBM & Oracle Java SDKs | Oracle JDK 9 | Computing platform to create, develop and run web-based applications | Application Development and Support | Licensure,  Infrastructure Support |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Application Development and Support | Licensure,  Infrastructure Support |
| WebSphere | Websphere Webserver | Websphere 8.5.5 | Web application server for hosting Java based websites | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Windows Server | Windows Server Operating System (OS) | Server 2016 | Hosting Agency Portal application | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| Oracle Exadata | Exadata Database Machine | X5 | On premise computing platform specialized for running the Oracle Virtual Machines. | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| Oracle DB | Oracle Database | 12C | On premise Oracle relational database to support application data | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| Apache | ApacheDS | Most recent | Embeddable Java directory server – maintains the role based access information for this system | Application Configuration and Support | Licensure, Infrastructure Support |
| **IMPACT Worker Portal** | | | | | |
| Java | IBM & Oracle Java SDKs | Oracle JDK 9 | Computing platform to create, develop and run web-based applications | Application Development and Support | Licensure,  Infrastructure Support |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Application Development and Support | Licensure,  Infrastructure Support |
| Eclipse BIRT | BIRT | 4.X | Reporting tool for access to IMPACT reports | Application Configuration, Development, and Support | Licensure, Infrastructure Support |
| Apache | ApacheDS | Most recent | Embeddable Java directory server – maintains the role based access information for this system | Application Configuration and Support | Licensure, Infrastructure Support |
| Microsoft LDAP | Microsoft Lightweight Directory Services (LDS) | N/A | Statewide LDAP supporting secure access for State-issued ID users, as well as service accounts | Maintenance of linkage to LDAP | Licensure, Infrastructure Support, and Configuration |
| WebSphere | WebSphere Webserver | WebSphere 9.0.0.7 | Web application server for hosting Java based websites | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Windows Server | Windows Server Operating System | Server 2016 | Hosting Agency Portal application | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| Oracle Exadata | Exadata Database Machine | X5 | On premise computing platform specialized for running the Oracle Virtual Machines | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| Oracle DB | Oracle Database | 12C | On premise Oracle relational database to support IMPACT system | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| **Document Center** | | | | | |
| Captiva | OpenText Captiva | 7.1 | Software for document information processing and data capture | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| .Net | Visual Basic .Net | Most recent | Object-oriented programming language implemented on the .Net framework | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| WebSphere | Websphere Webserver | Websphere 9.0.0.7 | Web application server for hosting Java based websites | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| IBM Content Manager | Content Manager Enterprise Edition | V 8.6 | Web content management application for all Eligibility & Enrollment and IMPACT documentation. | Application Configuration and Support. | Licensure,  Infrastructure Support |
| IBM | DB2 | DB2 11.1 | Microsoft Relational Database to support application data | Database Configuration and Support | Administrative DBA Support, Licensure,  Infrastructure Support |
| Windows | Windows Server Operating System | Windows Server 2012 | Server and operating system to support the Document Center | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| Apache | ApacheDS | Most recent | Embeddable Java directory server – maintains the role based access information for this system | Application Configuration and Support | Licensure, Infrastructure Support |
| Microsoft LDAP | Microsoft Lightweight Directory Services (LDS) | N/A | Statewide LDAP supporting secure access for State-issued ID users, as well as service accounts | Maintenance of linkage to LDAP | Licensure, Infrastructure Support, and Configuration |
| **Genesys Phone I3/IVR System (see Att J – I3-IVR Genesys PureConnect System Overview)** | | | | | |
| Genesys PureConnect | Genesys PureConnect Interaction Center  Genesys PureConnect IVR | 2018 R3 | Application Server Software required to support the DFR Phone System and contact center applications | Application Configuration, Development, and Support | Licensure,  Infrastructure Support, and Administration |
| Windows | Windows Server Operating System | Windows Server 2016 | Server and operating system to support Genesys software | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| SQL | SQL Server | SQL Server | Database server to support application data | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| Microsoft LDAP | Microsoft Lightweight Directory Services (LDS) | N/A | Statewide LDAP supporting secure access for State-issued ID users, as well as service accounts | Maintenance of linkage to LDAP | Licensure, Infrastructure Support, and Configuration |
| **CDMS** | | | | | |
| Java | IBM & Oracle Java SDKs | Oracle JDK 9 | Computing platform to create, develop and run web-based applications | Application Development and Support | Licensure,  Infrastructure Support |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Application Development and Support | Licensure,  Infrastructure Support |
| Oracle Exadata | Exadata Database Machine | X5 | On premise computing platform specialized for running the Oracle Virtual Machines | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| Oracle DB | Oracle Database | 12C | On premise Oracle relational database to support application data | Database Configuration and Support | Administrative DBA Support, Licensure, and  Infrastructure Support |
| WebSphere | Websphere Webserver | Websphere 9.0.0.7 | Web application server for hosting Java based websites | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Windows | Windows OS | Windows Server 2012 R2 | Operating system required to support CDMS. | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| Apache | ApacheDS | Most recent | Embeddable Java directory server – maintains the role based access information for this system | Application Configuration and Support | Licensure, Infrastructure Support |
| Microsoft LDAP | Microsoft Lightweight Directory Services (LDS) | N/A | Statewide LDAP supporting secure access for State-issued ID users, as well as service accounts | Maintenance of linkage to LDAP | Licensure, Infrastructure Support, and Configuration |
| **Benefits Portal** | | | | | |
| Java | IBM & Oracle Java SDKs | Oracle JDK 9 | Computing platform to create, develop and run web-based applications | Application Development and Support | Licensure,  Infrastructure Support |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Application Development and Support | Licensure,  Infrastructure Support |
| Undertow | Undertow Web Application Server | 2.0 | Embedded Java-based web server designed to be run within the Docker Containerization software | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Red Hat | Red Hat Enterprise Linux | RHEL 6 | Operating System for Unix | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure,  Infrastructure Support |
| Web Server | IBM HTTP Server | 9.0 | Web application server for the Benefits Portal | Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Docker EE | Docker EE for Redhat Enterprise Linux | 17.06 | Lightweight alternative to full machine virtualization that involves encapsulating an application in a container with its own operating environment | Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Mongo | Mongo DB | 4.0 |  | Configuration, Development, and Support | Licensure,  Infrastructure Support |
| Apache | Apache DS | Most recent | Embeddable Java directory server | Configuration, Development, and Support | Licensure,  Infrastructure Support |
| ELK | ELK Stack | Most recent | Monitor applicable application logs | Configuration, Development, and Support | Licensure, Infrastructure Support |
| **Other / Overall** | | | | | |
| Informatica | ETL and MongoDB connector | 10.2 | Extract, Transform, Load services between AS components and Data Warehouse | Configure and Maintain ETL processes within Informatica | Licensure, Infrastructure, Support, and Administrative Configuration |
| IBM COGNOS | COGNOS Reporting Studio / Analytics | 11 | Supports access to AS Reports | Provide the data and reports to Data Warehouse for them to create and/or post reports | Licensure, Infrastructure, Support, Administrative Configuration, and COGNOS Reporting Studio use |
| Nagios | Core | Most recent | Monitoring servers in the AS solution | Configuration and Support | Licensure, Infrastructure, Support, Administrative Configuration |
| IOT NOC and SOC monitoring tools | Multiple toolsets and technologies | N/A | Monitor network and security infrastructure | Review reporting, alerts, notifications, and other relevant data to manage all AS solution components. | Licensure, Infrastructure, Support, Administrative Configuration. Provide NOC/SOC services to all AS infrastructure. |
| Rational | RPT  Jazz | Most Recent | RPT for automated performance testing.  Jazz for Application Lifecycle Management (ALM). | Use RPT, as applicable, for performance testing.  Maintain up to date SDLC requirements, design, testing, and other related artifacts. | Licensure, Infrastructure, Support, Administrative Configuration. Provide role based access. |
| Jenkins | Jenkins | Most recent | Build / deployment tool | Use Jenkins, among other build tools, to build and maintain applicable AS components. | Licensure, Infrastructure Support. |
| Atlassian | JIRA | Most recent | Requirements and testing tracking tool for ALM purposes. | Maintain up to date SDLC requirements, design, testing, and other related artifacts. | Licensure, Infrastructure, Support, Administrative Configuration. Provide role based access. |
| Microsoft Office 365 SharePoint | Microsoft Office 365 SharePoint | Most recent | AS document repository to support all aspects of Contractor’s artifact management | Maintain PM and SDLC artifacts. Clarify access changes to State so that State SharePoint administrator can provide, delete, or modify permissions for Contractor staff. (No PII/PHI data to be stored.) | Licensure, Infrastructure Support. (No PII/PHI data to be stored.)  Collaborate with Contractor on artifacts as applicable. Administer role-based access. |
| Windows | Windows Server | Windows Server 2016 | OS to support existing OPEX Scanners | Understanding of middleware, database, and other application components’ interaction with the OS / Monitor Security Scanning results from IOT; support the State in identifying Application/software vulnerabilities and mitigations; support the State in managing baseline secure configuration | Licensure, infrastructure support |

**Workstation Tools / Technologies** (Generally speaking, unless noted below, the Contractor is responsible for their own workstations, applicable workstation hardware/software licensure, and applicable infrastructure support. The State is responsible for the licensure of State-owned components, but the Contractor is responsible for AS components functioning correctly with applicable State-owned components.)**:**

| **PC / workstation Software** | **Tool / Technology** | **Version** | **Brief Description of the Purpose** | **Contractor Responsibility** | **State Responsibility** |
| --- | --- | --- | --- | --- | --- |
| **Agency Portal - Contractor** | | | | | |
| Windows | Windows Operating System | Windows 10 | Operating system to support agency applications. | Licensure and infrastructure support for Contractor workstations | None |
| Browser | Firefox, Chrome, Edge, or Internet Explorer (IE 11 and on), and also Mobile OS browsers (Android Chrome, iOS Safari) | Latest version of the browsers supported | Internet browsers needed to access the Agency Portal, system is browser agnostic | Licensure and infrastructure support for Contractor workstations | None |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Licensure and infrastructure support for Contractor workstations | None |
| **Agency Portal – End User (Agencies)** | | | | | |
| Browser | Firefox, Chrome, Edge, or Internet Explorer | IE 11 or newer, latest Chrome (including mobile), and latest Firefox | Internet browsers needed to access the Agency Portal, system is browser agnostic | Solution to support the use of these browsers | For workers, provide workstation browser support, including group policy and patch management |
| **IMPACT Worker Portal - Contractor** | | | | | |
| Windows | Windows Operating System | Windows 10 | Operating system to support agency applications. | Licensure and infrastructure support for Contractor workstations | None |
| Browser | Firefox, Chrome, Edge, or Internet Explorer | IE 11 or newer, latest Chrome, and latest Firefox | Internet browsers needed to access the Eligibility Worker Portal, system is browser agnostic | Licensure and infrastructure support for Contractor workstations | None |
| Eclipse BIRT | BIRT | 4.X | Reporting tool for access to IMPACT reports | Application Configuration, Development, and Support. Licensure, Infrastructure Support | Server infrastructure support |
| **IMPACT Worker Portal – End User (DFR E&E and IMPACT Workers)** | | | | | |
| Windows | Windows Operating System | Windows 10 | Operating system to support agency applications. | Solution to support the use of this OS using the browsers noted below | Licensure,  Infrastructure Support |
| Browser | Firefox, Chrome, Edge, or Internet Explorer | IE 11 or newer, latest Chrome, and latest Firefox | Internet browsers needed to access the IMPACT Worker Portal, system is browser agnostic | Solution to support the use of these browsers | Support and Maintenance |
| **Document Center - Contractor** | | | | | |
| Windows | Windows Operating System | Windows 10 | Operating system to support agency applications. | Licensure and infrastructure support for Contractor workstations | Licensing, Patching / Maintenance |
| Captiva | OpenText Captiva | 7.1 | Software for document information processing and data capture | Application Configuration, Development, and Support | Licensure,  Infrastructure Support |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Document Center – End User (DFR Document Processing Workers)** | | | | | |
| Browser | Firefox, Chrome, Edge, or Internet Explorer | IE 11 or newer, latest Chrome, and latest Firefox | Internet browsers needed to access the Doc Center, system is browser agnostic | Solution to support the use of these browsers | Support and Maintenance |
| Windows | Windows Operating System | Windows 10 | Operating system to support agency applications. | Solution to support the use of this OS using the browsers noted above | Licensing, Patching / Maintenance |
| Captiva |  | 7.1 | Software for document information processing and data capture | Application Configuration, Development, and Support. Support Document Center staff with technical issues, as applicable | Licensure,  Infrastructure Support |
| Adobe | Adobe Acrobat and / or Adobe Reader | Latest version available | Family of application software and Web services developed by Adobe Systems to view, create, manipulate, print and manage files in Portable Document Format | Support the loading of TIFFs and PDFs into Document Center solution | Licensing, Maintenance and Support |
| OPEX Scanners | OPEX Scanner | Falcon and Falcon RED | High volume scanners used to process all documents submitted to DFR Document Center. Jobs on these scanners interact with Captiva. | Ensure OPEX Scanners jobs are supported, including the interaction with Captiva. Support Document Center staff with technical issues, as applicable | Licensure,  Infrastructure Support |
| Multifunction Printers (MFPs) | Ricoh | N/A | MFPs set up in State Local Offices (LOs) used by workers and clients to scan in documents, including barcoded documents | Support, with Ricoh, the assurance of documents routed to the Document Center correctly to applicable processing queues, including indexing to cases | Licensure, Infrastructure Support / Agreement with Ricoh |
| **Genesys Phone I3/IVR – Contractor (see Att J – I3-IVR Genesys PureConnect System Overview)** | | | | | |
| Genesys Pureconnect | Interaction Desktop,  Interaction Center Business Manager,  Interaction Administrator,  Interaction Attendant  Interaction Log Viewer | 2018 R3 | Application software required to support the DFR Phone System and contact center applications | Development, Configuration, and Support of Att J noted components | Licensing, Configuration, Maintenance and Support |
| Windows | Windows Operating System | Windows 10 | Operating system to support Genesys software | Licensure and infrastructure support for Contractor workstations | None |
| SDK | Microsoft .Net Framework SDK | 4.7 | Software Development Kit to create, develop and run applications in Windows and .Net Framework | Development and Configuration. Licensure. | None |
| Multimedia Processing | AVS4You | 8.5 | Audio recording, editing, and enhancing software to support updates to IVR Prompts | Configuration | Licensing and Support |
| SQL Server Studio | Microsoft SQL Server Management Studio | 17.8 | Database access tool for configuring, managing, and administering components within Microsoft SQL Server | Configuration and Administration. Licensing and Support | None |
| **I3/IVR – End User (DFR Workers using Genesys client to answer calls)**  **(note: clients, ARs, and agencies are end users as well, but only via phone)** | | | | | |
| Genesys Pureconnect | Interaction Desktop,  Interaction Center Business Manager,  Interaction Administrator | 2018 R3 | Application software required to support the DFR Phone System and contact center applications | Development, Configuration, and Support | Licensing, Configuration, Maintenance and Support |
| Windows | Windows OS | Windows 10 | Operating system to support Genesys software | Solution to support the use of this OS for workers | Licensing, Patching / Maintenance |
| **CDMS - Contractor** | | | | | |
| Windows | Windows OS | Windows 10 | Operating system to support CDMS application | Licensure and infrastructure support for Contractor workstations | None |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Licensure and infrastructure support for Contractor workstations | None |
| Jenkins | Jenkins | Most recent | Automation server to build and Deployment tool | Licensure and infrastructure support for Contractor workstations | Licensure |
| **CDMS – End User (E&E Workers)** | | | | | |
| Browser | Firefox, Chrome, Edge, or Internet Explorer | IE 11 or newer, latest Chrome, and latest Firefox | Internet browsers needed to access the Doc Center, system is browser agnostic | Solution to support the use of these browsers for workers | N/A |
| Windows | Windows OS | Windows 10 | Operating system to support CDMS application | Solution to support the use of this OS for workers with browsers noted above | Licensing, Patching / Maintenance |
| Adobe | Adobe Acrobat and / or Adobe Reader | Latest version available | Family of application software and Web services developed by Adobe Systems to view, create, manipulate, print and manage files in Portable Document Format | Solution to support the use of this platform for accessing, modifying, and uploading TIFFs and PDFs | Licensing, Maintenance and Support |
| **Benefits Portal – Contractor** | | | | | |
| ALM | Atlassian Jira ALM | Most recent | Application Lifecycle Management | Configuration for SDLC | Licensure and Support |
| Mongo DB | PowerExchange for MongoDB  MongoDB Enterprise Advanced | Most recent | Database and tools for New Client Benefits Portal | Configuration, vulnerability monitoring, patching, baseline configuration maintenance | Licensure and Support |
| Jenkins | Jenkins | Most recent | Automation server to build and Deployment tool | Licensure and infrastructure support for Contractor workstations | None |
| Java | Spring Framework | N/A | Java framework for developing, building and deploying web-based enterprise applications online | Licensure and infrastructure support for Contractor workstations | None |
| **Benefits Portal – End Users (clients, ARs, agencies)** | | | | | |
| Browser | Firefox, Chrome, Edge, or Internet Explorer (IE 11 and on), and also Mobile OS browsers (Android Chrome, iOS Safari) | Latest version of the browsers supported | Internet browsers needed to access the Benefits Portal, system is browser agnostic. | Solution to support the use of these browsers | None |
| Adobe | Adobe Acrobat and / or Adobe Reader | Latest version available | Used to access documents (via browser) provided to users on the Portal | Solution to support the access of documents via browser/Adobe | None |
| **Other / Overall** | | | | | |
| IOT Network Operations Center (NOC) and Security Operations Center (SOC) tools | N/A | N/A | These NOC and SOC tools will monitor interaction with network and State-hosted servers/devices. These tools include Web Server and Firewall appliances/solutions. | Address security and network incidents identified by the State. Work with the State to monitor applicable firewall rules associated with AS components, including the recommendation of secure firewall rules for prod and non-prod. | Licensure, Infrastructure Support, and Firewall Management |
| Contractor-identified software to support scope in this RFP | N/A | N/A | These tools and technologies may be necessary above and beyond what is listed throughout this RFP to optimally support State’s required AS solutions and goals | Licensure and Infrastructure Support | None |
| Application Vulnerability and Assessment Tools | Static and Dynamic Scanning,  Code Quality Assessment tools, and infrastructure vulnerability assessment tools | Contractor’s Discretion, pending State approval | These tools and technologies are used in support of security compliance noted throughout this RFP | Licensure and infrastructure support for Contractor-led application vulnerability assessment, code quality assessment, and infrastructure vulnerability assessment of Contractor managed components.  Support State-executed and/or 3rd party audits of application vulnerability, code quality, and infrastructure vulnerability.  Address and manage vulnerabilities, with reporting to the State, including support on federal reporting, regardless of entity who has assessed and provided findings. | State-conducted application vulnerability, code quality, and infrastructure vulnerability assessments. Provide applicable findings to Contractor for them to address. Ultimate responsibility lies with the State to provide applicable federal reporting |
| Adobe | Adobe Acrobat and / or Adobe Reader / Adobe DC / Adobe Pro | Latest version available | Support workers’ access to PDFs, including the manipulation of PDFs and other documents (e.g., TIFFs, Word documents) in preparation of documents that are loaded to CDMS and other systems, as applicable | Understand the use of Adobe tools in the environment to generate PDFs uploaded to CDMS. Contractor to provide licensure and support to Contractor staff, as applicable | Licensure, infrastructure support for State-owned workstations |

The Contractor shall manage the servers utilized for the execution of the Contract duties. As of January 2019, there are 349 servers being managed under the current contract (268 servers after subtracting legacy components that will be decommissioned, as noted above (i.e., Cúram and Adobe Livecycle components). Provided in the table below is a snapshot of the breakdown by operating system, purpose, and service/program. The total quantity and breakdown of quantities is subject to change before Contract execution and during the term of the Contract. All of this infrastructure is hosted by IOT.

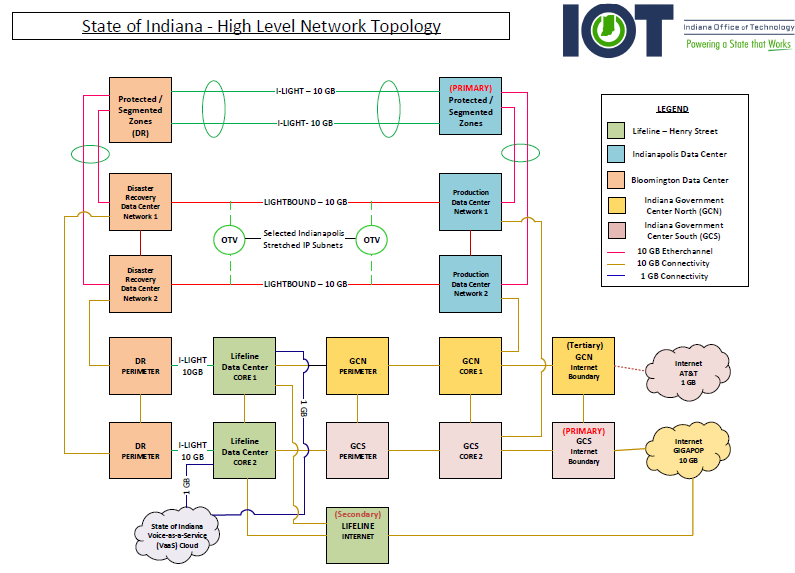
Generally speaking, the incumbent vendor SDLC includes the following flow of code and configuration promotion through servers: Unit (Development) -> System Integration Testing (SIT) -> Integration Testing (INT) -> User Acceptance Testing (UAT) / Performance Testing (PERF) / Training (TRN) -> Staging (STG) -> Production (PRD). Some servers may serve multiple purposes (e.g., Dev + SIT on one server or UAT + PERF on one server). Additionally, not all of AS components may need to flow through this mix of servers to optimally support the SDLC. Lastly, a number of these servers may be serving in a Disaster Recovery (DR) capacity at the Bloomington, IOT-supported, Datacenter. These in-depth details, per server, will be provided to the Contractor during Contract negotiation. At a summary level, out of 268 servers:

|  |  |
| --- | --- |
| **Breakdown by Operating System** | * Windows Server (2008, 2012, or 2016) – 247 * Redhat Enterprise Linux - 21 |
| **Breakdown by Purpose** | * Development - 60 * System Integration Testing - 33 * Integration Testing - 11 * UAT – 81 * Training - 9 * Production - 74 |
| **Breakdown by Service/Program** | * Server that support all the AS solution (e.g., jump servers, LDAP, web servers supporting multiple components) – 22 * Benefits Portal/Agency Portal - 26 * Document Center - 146 * CDMS – 33 * IMPACT - 14 * I3-IVR – 27 (as noted in Att. J, these servers are handled by IOT and the Contractor together) |

* + 1. **IOT Datacenter Infrastructure for the AS Solution**

The IOT Datacenters support all AS solution component hosting and will support the Contractor’s secure access to servers and other applicable AS solution components.

The below diagram describes the current network connections for the Production system. There is one Production datacenter in Indianapolis, IN and the Disaster Recovery (DR) datacenter is in Bloomington, Indiana. The Contractor is required to support the AS DR solution using the infrastructure at the Bloomington DR site.



# **Scope of Services Overview**

The State is seeking to establish a contract for both AS M&O and enhancements services through this contract. Below is a high-level description of these two types of services, along with the Contractor’s responsibilities. Please see Section 6 for more details of the M&O workstreams and Section 7 for more details of the enhancements process.

* 1. **M&O Services.** There are six (6) M&O workstreams in the scope of this Contract.

1. Benefits Portal M&O

2. Agency Portal M&O

3. CDMS M&O

4. Document Center M&O

5. IMPACT M&O

6. I3/IVR M&O

The Contractor shall provide the following services for all M&O workstreams and enhancements. Please see Section 6 for additional details for these services.

* **Architecture Services** (See Section 5.1)
* **SDLC Services** (See Section 5.2. See Section 5.3 for Testing and defect management details)
* **SDLC Artifact Management** (See Section 5.4)
* **SDLC Quality Management** (See Section 5.5)
* **Software/Hardware Management** (See Section 5.6.1)
* **Infrastructure Management** (See Section 5.6.2)
* **Application Lifecycle Management (ALM)** (See Section 5.6. 3)
* **Database Support** (See Section 5.6. 4)
* **Application Monitoring** (See Section 5.6.5)
* **Incident Management and Helpdesk Support** (See Section 5.6.6)
* **Access Management** (See Section 5.6.7)
* **Business and Operations Reporting** (See Section 5.7)
* **Security & Privacy** (See Sections 5.8 and10.1)
* **Solution M&O Services** (See Section 6 for all M&O workstreams)
* **DDI, Enhancements, and Change Management** (See Section 7)
* **Training** (See Section 8)
* **Transition and Turnover** (See Section 9)
* **Business Continuity and Disaster Recovery** (See Section 10.2)

Additionally, the Contractor shall provide business and technical subject matter expertise on all aspects of the AS solution and processes. The State has policy, operations, and business SMEs who are Managers, Business Analysts, System Analysts, Technical Managers, Technical Analysts, and other related staff. Some of these staff may come from partner systems, agencies, or other applicable interface partners. These individuals must be consulted on design, defect triage, system operational issues, and system direction. These specific individuals will be made clear to the Contractor upon engagement. In terms of governance, the State is the ultimate decision maker on all aspects of AS solution management, including Change Management.

* 1. **Enhancements.** The DDI for enhancements shall be conducted according to the Contract’s SDLC processes. Enhancements can be for new AS solution components or enhancements and/or configuration changes to existing AS solution components. These modifications will be managed via the Change Management process. One example of an anticipated enhancement that falls under the scope of this contract is the IBM Content Manager replacement for Document Center. Please see Section 7.10 for additional information on this enhancement.
  2. **Staff Skills Overview.** The Contractor is expected to use individual staff to cover multiple M&O services and enhancement efforts to the greatest extent possible, while not sacrificing quality of service, including service level agreements (SLAs). These services are not anticipated to be provided in “silos”, and the Contractor should find efficiencies in staffing. The Contractor will provide staff for the following areas, as needed to successfully execute the scope of this Contract:
* **Architecture** (applies to all scope, with special focus on DDI for enhancements). See Architect roles in Attachment I
* **Program/Project Management** (applies to all scope)
  + See Program Manager and Project Manager roles in Attachment I
  + Note: Program Managers may be responsible for different areas noted in this section (e.g., “Business Analysis Program Manager”, “Development Program Manager”, and “Testing Program Manager”)
* **Business Analysis** (applies to all scope). See Business Analyst roles and User Interface (UI) Specialist role in Attachment I
* **Development** (applies to all scope). See Developer roles in Attachment I
* **Testing** (applies to all scope). See Tester roles in Attachment I
* **Technical** (applies to all scope). See Database Administrator (DBA), Operations Support, IT Program Director, Systems Analyst, and WebSphere/Apache Administrator roles in Attachment I
* **Reporting** (applies to all scope). See Developer – Metrics, Developer – Cognos, and Business Analyst/Tester – Metrics roles in Attachment I
* **Security** (applies to all scope). See Chief Information Security Officer and Senior Information Security Specialist roles in Attachment I as well as several other roles that require privacy & security backgrounds (e.g., Business Analysts, Developers, Testers, and Technical staff)

It is important to the State that services to clients and workers are not interrupted by changes to the AS solution. As such, the Contractor shall ensure that clients, workers, and other AS solution end users are not adversely impacted by the DDI of any system change requests, including enhancements.

The State is dependent on the Contractor for providing products and services that fully comply with the requirements and deliverables set forth in the contract. State approval of the Contractor’s work product associated with the responsibilities, requirements, and deliverables does not in any way relieve the Contractor from full financial responsibility should the Contractor’s work product not meet the State requirements, as set out in the RFP and the subsequent contract.

Note: Upon request, the State or Federal partners will be granted access to the AS solution and contract-related cost records of the Contractor and subcontractors.

* 1. **Operational Verification and Validation (OV&V) Vendor.** DFR has contracted with an OV&V vendor to help review AS changes (e.g. solution changes, report configuration changes, etc.). They will provide checkpoints during SDLC that allow the SDLC process to move forward: Change Requests (CRs); Requirements; Design, Development, and Testing; and Implementation. They also will conduct a Post Implementation Review to ensure the change is working as expected, all documentation is correctly stored, and any post implementation defects are properly addressed. Additionally, they will track predefined SLAs of the Contractor regularly to monitor and report on Contractor performance.
  2. **Independent Verification and Validation (IV&V) Vendor.** DFR has also contracted with an IV&V vendor to assist with IEDSS scope. As this Contract pertains to some IEDSS scope (e.g., interfaces with the IEDSS Worker Portal and creation of replacement solution components for the Benefits Portal and Document Center), the Contractor will be expected to share SDLC status with the IV&V vendor.
  3. **Maintenance Releases (MRs) and Change Requests (CRs).** The Contractor will employ periodic MR and non-MR for promotion of configuration and development artifacts to production. Each MR is a collection of Change Requests (CRs) (enhancements, changes, and configuration updates) and defects fixes, with indexed reference numbers tracked by the State’s ALM tool. Non-MR promotions to production are individual CRs or defect fixes, also tracked via indexed reference numbers from the ALM.

# **Project Management**

* 1. **Project Management Standards**

Overall decision governance structure and prioritization of tasks, issue resolutions, and risk mitigations will be set and managed by DFR; however, AS Program and Project Management staff will have a role in managing each of these components within the scope of AS, while providing status and escalation to DFR and the State as appropriate. The Contractor is expected to support the State in maintaining an efficient and effective decision governance structure by providing best practices and/or insights from previous experience maintaining and operating a solution similar in size and scope as the AS solution.

The Contractor must develop an overall Project Management Plan (deliverable created within 30 days after Contract begins) and approach that adheres to the guidelines established by the State. The Contractor’s Project Management Plan must also adhere to the IOT Project Review Policy, found at <https://www.in.gov/iot/files/project_review_policy_20110311_final.docx>.

From the CMS MEET, the Contractor must provide the following services with Program/Project Management for DDI efforts, and maintain these concepts under M&O scope:

* Planning Services
  + Vision, strategy, assistance in developing goals and objectives
  + Concept of Operations
  + Enterprise functional and non-functional needs analysis
  + Continuity of operations and disaster recovery planning
  + Architectural & engineering decomposition
  + Communications planning
  + Organizational change management, identify stakeholders and owners for each module and business area, assess stakeholder and owner needs, measure change adoption, administer reinforcement mechanisms
* Management Framework Services
  + Enterprise design, pattern and portfolio management
  + Enterprise architecture, modelling and integration
  + Enterprise technical roadmap orchestration with sequencing and transitioning plan
  + Enterprise functional and non-functional requirements
  + MITA strategy, align to-be and Standards and Conditions for Medicaid IT goals to module integration and certification plans, validate plans against MITA Maturity Roadmap, identify deviations from MITA strategy, manage issues and communication with MITA business process owners
  + Development life cycle
  + Enterprise management of master integrated schedule, scope, change control, risk management, and quality assurance
* Functional Implementation Services
  + Standards selection
  + Master data management, identity, and access management
  + Document management
  + Integration services
  + Business architecture and modeling, business rules engine
  + Information architecture and modeling
* Technical Implementation Services
  + Environment / infrastructure
  + Network services
  + Portal, module portal
  + Enterprise service bus, adapters, meta data repository, transfer engine, process orchestration engine, dashboard, batch engine
  + Identity management
  + Platform services layer, data services layer, master data
  + Enterprise services registry
  + Standards selection
  + Security architecture and framework
  + Application Programming Interface (API) management and governance, publish and promote APIs, automate and control connections, monitor traffic, provide memory management and caching mechanisms, manage governance platform, API subscriptions, API promotion meta-data and design checkpoints and synchronize with Service-Oriented Architecture (SOA) governance and business strategy and goals
* Module Integration
  + Advise source selection committee, assess modules for fit within enterprise architecture (EA) and integration platform,
  + Validate open APIs and standards, fit/gap assessment documentation, inform configuration-over-customization decisions throughout project life cycle
  + Develop master data conversion, migration and test plans and associated procedures and standards,
  + Define test acceptance criteria and standards enforcement,
  + Oversee module vendor integration and deployment activities,
  + Assist in module integration as required for modules vendors without sufficient native integration capabilities
* Certification Involvement
  + Participate in and support certification activities with State, CMS, and IV&V, and monitor necessary modifications

From FNS, the SNAP Review of Major Change in Program Design and Management Evaluation Systems (<https://www.fns.usda.gov/snap/fr-011916>) (also see 7 CFR 272.15 - https://www.law.cornell.edu/cfr/text/7/272.15) and Test Plan requirements (as part of FNS Handbook 901 and 7 CFR 277.18 (see https://www.law.cornell.edu/cfr/text/7/277.18) are applicable to the Contractor. While addressing a major enhancement, the Contractor shall support DFR in completing Major Change and Test Plan documentation, as applicable for the “Major Change”. While DFR will own and be responsible for documentation submitted for review to FNS, the Contractor will be expected to provide content as directed by DFR and also address any questions, concerns, or corrective actions that FNS indicates throughout their review or during SDLC activities.

* 1. **Project Plan Components**

The Contractor shall develop a Project Management Plan (PMP) that addresses execution of their scope of work, in alignment with State and Federal requirements (CMS and FNS noted above). The Project Management Plan shall be developed according to industry standards and best practices including the Project Management Institute’s (PMI) latest Project Management Body of Knowledge (PMBOK) and IEEE system and software processes where applicable. Once the Project Management Plan is approved by the State, the Contractor shall maintain and modify the approved Project Management Plan throughout the project by updating it to reflect the evolving schedule, priorities, and resources (i.e., it is a living document). At a minimum, the Project Plan shall include:

* Project Schedule Management Plan
  + High level schedule for term of contract
* Project Organization and Resource and Staffing Plan, along with key personnel by name, title and job function, and whether the personnel are Contractor or subcontractor employees
* SDLC Management Plan
* Configuration Management Plan
* Issue Management Plan
* Risk Management Plan
* Communication Plan
* Quality Assurance Measures
* Descriptions of any tools that the Contractor will use to manage any component of the Project Management Plan
* MITA Maturity Improvement Plan

The Project Management Plan must be provided to the State within thirty (30) days of the Contract start date. Following required State approval of the PMP, the Contractor must review the PMP monthly to determine if any updates are required. The State or the Contractor may request changes at any time to the PMP, but the Contractor and the State must mutually agree upon any updates.

* 1. **Status Updates**

The Contractor shall meet with the State weekly to provide project updates (see Management Reporting in Section 4.5). The Contractor shall submit Weekly Status Reports that include updated risk logs with risk mitigation strategies, issues logs, and the latest approved Project Schedule and status updates. The Contractor shall review these reports during the weekly update meetings.

The Contractor shall also attend any ad hoc meetings requested by the State. If on-site attendance is necessary, the State will provide advanced notice. See Attachment I for staff who are required to be available in Indianapolis for meetings. If presentation material is necessary, the Contractor shall develop the materials.

* 1. **Project Quality Management**

The Contractor shall employ quality management to monitor and control project quality to achieve a high level of customer satisfaction with delivered products and services. The Contractor’s quality management approach shall serve several purposes:

* Defines the approach to verify that project methods, processes, templates, and tools are being used by the project team properly and are effective.
* Defines the approach to verify that deliverables are meeting project standards and quality expectations.
* Defines what additional groups outside the core project team will be supporting the project to help achieve these quality objectives.

**Quality Objectives and Standards.** The Contractor shall employ quality standards that measure the quality of their services and also alert the Contractor and State management to when the Contractor may be at risk of not meeting requirements and service level agreements. Examples of quality standards include measuring the number of software bugs per component, defining the most effective way to write a requirement, and measuring the length of time it takes to complete a document review. The quality objectives for this Contract include:

* Implementing mechanisms to satisfy the State’s AS solution expectations
* Documenting and adhering to project-wide standards
* Proactively avoiding issues by mitigating risks
* Reporting and evaluating performance measures

**Quality Management Planning.** The Contractor shall conduct the following to enable Quality Management:

* Quality Planning – Identify quality standards and measurements that are relevant to the project, and if not incorporated will result in low quality results. Determine how to satisfy each quality standard via the project schedule, resourcing and internal procedures. Develop a Quality Management Plan and continually update it throughout the Contract to incorporate lessons learned and modified standards and/or processes.
* Quality Assurance - Perform activities to verify that the project is using the proper methods, templates, standards, and guidelines, as well as practicing the right processes to produce high-quality deliverables that satisfy project requirements.
* Quality Control – Review Contract results to determine whether they meet expected standards and requirements and implement corrective actions or improvements when they do not. Produce the metrics used to monitor project status report and have Contractor leadership address delinquencies and negative trends.

**Implementing the Quality Management Plan.** Each Contractor team member shall be familiar with the quality processes using the methods listed below:

* Quality Assurance / Quality Management Plan Walkthrough – Upon approval of the Quality Management Plan, the Contractor will conduct a training session for all Contractor and State team members to provide an overview of the Quality Management Plan and will emphasize the importance of quality processes. Additionally, the Quality Management Plan will be included as one of the onboarding documents for new Contractor team members.
* Project Standards – An onboarding packet will be provided to each Contractor team member and will include, but is not limited to, the following standards as appropriate for their role:
  + Documentation standards
  + Document control standards
  + SDLC standards
  + Requirements standards
  + Coding standards
  + Testing standards
  + Configuration standards
  + M&O standards

**Deliverable Management.** The Contractor shall employ deliverable management activities to draft, review and obtain appropriate levels of State approval for Contract deliverables. Deliverables are required outputs for Contract work, such as management reports (see Section 4.5) and SDLC deliverables (see Section 5.2).

* The Contractor will submit electronic copies of all deliverables, including non-written deliverables (e.g., source code and software and network configurations) for each task or subtask. Each deliverable submitted to the State for review and approval will have a formal transmittal letter from a Contractor Project Manager.
* The Contractor is responsible for validating that Contractor staff uses the appropriate, approved templates and project tools for deliverables.
* The Contractor shall submit deliverables that are complete, meet all contract requirements, and on time per the approved Project Schedule.

The deliverable management process is detailed below:

* **Perform Deliverable Expectations Document (DED) Review** – The Contractor shall create the DED to define expectations and content for each deliverable. Note: The State may choose to waive the requirement for a DED and DED review for any specific deliverable.
* **Develop Draft Deliverable** - The Contractor shall create the draft deliverable after approval of the DED (including any applicable review criteria).
* **Deliverable Walkthrough** - The Contractor team shall conduct a formal deliverable walkthrough with appropriate State stakeholders. This review is critical in validating whether the agreed upon structure and content of the deliverable has been achieved.
* **Submit Deliverable** - The Contractor shall submit the deliverable by the approved deadline. The deliverable will comply with agreed upon standards and include the content described in the DED.
* **Review Deliverable** - The State will conduct deliverable review(s). The OV&V may also participate in the deliverable review process, and in such cases, the Contractor shall provide the OV&V with any information requested. The Deliverable Feedback Form (DFF) will be used to plan the deliverable reviews, as well as document the feedback gathered and track the follow-up required to resolve any defects.
* **Deliverable Acceptance and Approval** - Each final deliverable review will result in a written notice, via the Deliverable Acceptance Form, of a decision indicating deliverable acceptance or non-acceptance.

**Corrective Actions**

Quality defects identified during an internal quality review or at any other point during the Contract (e.g., by the State project manager) needs to be addressed quickly and tracked to closure. The Contractor shall document all quality defects identified during the quality assurance or quality management processes by request types (issues, risks, action items, changes, etc.) in the Contractor’s tracking tool. Additionally, the Contractor Project Manager will take responsibility for resolving any non-compliance with quality standards.

* 1. **Management Reporting**
     1. **Status and Performance Reports**

**Recurring Management Reports**

* **Overview:** TheContractor shall submit the following four (4) weekly management reports addressing the status of maintenance releases and non-maintenance releases. The first two (2) are Maintenance Release (MR) Status Reports (an MR is a – collection of CRs and defect fixes). These can be broken down by Sprint status, if the SDLC process includes this approach. There can be several concurrent MRs, and a report for each active one (i.e., planning and requirements have commenced) must be made available weekly for discussion with DFR, OV&V, and other applicable stakeholders.
  1. MR Report Type 2 – CRs and defect fixes (including those applicable to IEDSS interfaces) applicable to the following:
     + Benefits Portal
     + Agency Portal
     + Document Center (can include status on Content Manager replacement DDI)
     + I3/IVR
     + CDMS
  2. MR Report Type 3 - CRs and defect fixes applicable to IMPACT
  3. Security Status Report
     + Security status for all AS solution components, with updates on assessments, defect fixes, security testing, and mitigation activities for all scope.
  4. Non-Maintenance Releases Report
     + One report with all CRs and defect fix status that fall within this category
* **Management Report Content:** 
  1. The following fields must be covered in the MR Status Reports:

|  |
| --- |
| * **Project Status** * **Listing of DFR, IOT, and FSSA sponsors** * **AS Project Manager** * **Project Description** * **Project Benefits** * **Key Updates, Critical Issues, Risks and Mitigations**   1. General Status   2. Key Updates * **Requirements Status (depends on the MR and timing)** * **Red/Yellow/Green Status for Schedule, Quality, and Cost (Resource Utilization/Availability)** * **Status by Scope Items (content depends on the MR)** * **Milestone Summary**    1. Milestone   2. Plan Start Date   3. Estimated/Actual Start Date   4. Plan End Date   5. Estimated/Actual End Date * **Open Issues**    1. Description   2. Created By   3. Date Created   4. Resolution Target Date   5. Date Last Updated   6. Status   7. Impact   8. Assigned To   9. Resolution/Note**s** * **Initial Resource Estimates (Hours) by Resource Type and Actuals expended so far**   1. Project Management   2. Business Analysis   3. Development   4. Testing   5. Technical   6. Other * **SLA Compliance Status (See Section 12)** * **Testing Status (Defect and Fix Status) in alignment with FNS Test Plan requirements** |

* 1. The following fields must be covered in the Non-MR Status Report:

|  |
| --- |
| * **Listing of DFR, IOT, and FSSA sponsors** * **AS Project Manager** * **Key Updates, Critical Issues, Risks and Mitigations** * **Status by Scope Items**   1. Item #   2. Scope Item Title   3. Jazz #   4. Project Phase   5. State Approved Change Request Type   6. Status   7. Target Implementation Date   8. Initial Resource Estimates (Hours) by Resource Type and Actual Resources expended so far      + Project Management, Business Analysis, Development, Testing, Technical, Other * **Accomplishments for this Reporting Period**   1. Completed   2. Planned, Not Completed * **Planned Accomplishments for Next Reporting Period** * **SLA Compliance Status (See Sections 12)** * **Testing Status (Defect and Fix Status) in alignment with FNS Test Plan requirements** |

**Ad Hoc Reports**

The Contractor shall develop ad hoc status reports at the request of the State, with a ten (10) business day turnaround day unless otherwise specified by the State.

* + 1. **Task and Hours Tracking**

For the purposes of cost allocation across the multiple users and funding sources for this Contract, the Contractor shall track the time spent by each team member. Fields will include:

* Staff member name
* Task / Justification of Hours Expended
* Hours
* Change Request (if applicable)
* MR number (if applicable)
* Program (may be able to indicate this via CR / task information as denoted during initial Steering Committee direction for the funding of the CR)

The Contractor shall submit this information in a clear report with each invoice. The Contractor shall develop and maintain a tool to track this information and work with the State to finalize the reporting format and content. The State will allow the Contractor to determine the best tool to generate the required content. For example, the tool may be an Excel file, or it can be a module within a time tracking/HR tool. The State may audit the Contractor’s compliance with the Contract, including these Task and Hours Tracking requirements. Consequently, using and maintaining a tool for these tracking purposes can streamline audit assessment activities, if the process and system are well maintained.

# **AS Services for All M&O Workstreams and Enhancements**

The Contractor is expected to use the Project Management and SDLC concepts from Section 4 and Section 5.2 above to provide the AS M&O and enhancements services described in this section.

See Section 11 below for further information on staffing to support these AS services and see Attachment I for a listing of individual positions that the Contractor must use to support these AS services.

The Contractor is expected to use individual staff to cover multiple M&O services and enhancement efforts to the greatest extent possible, while not sacrificing quality of service, including SLAs. These services are not anticipated to be provided in “silos”, and efficiencies in staffing are expected.

* 1. **Architecture Services**

High level software and hardware components are included in Section 2.6 with high level architecture diagrams noted in Attachment J. The Contractor is expected to use best practices for system architecture while complying with applicable Federal requirements, including MITA.

The Contractor must support the State in maintaining the MITA maturity status for the AS solution. As enhancements, including DDI efforts progress throughout the term of the Contract, the Contractor is expected to provide recommendations and support MITA maturity improvements.

The Contractor is expected to maintain existing architecture artifacts. Additionally, they must update these artifacts and generate new architecture artifacts, as applicable, throughout the SDLC process.

* 1. **Software Development Lifecycle (SDLC) – Requirements and Process**

The Contractor shall follow a standard SDLC process to maintain AS solution components, including applying the process to the execution of DDI activities to execute CRs for defect fixes and enhancements. The Contractor’s approach must incorporate iterative methods for development and testing of software and training. The State and the OV&V Contractor will monitor compliance with these standards and address consistently poor performance.

For each meeting with program areas and other stakeholders, the Contractor will be responsible for coordinating logistics, preparing the meeting agenda, documenting, and publishing meeting notes and action items.

The SDLC method used historically on this project has been Waterfall with concepts incorporated from Waterfall/Agile/Scrum/Kanban methodologies. These approaches have been in support of AS solution components architected via traditional Service Oriented Architecture (SOA) or microservices. The table below contains the required minimum deliverables by SDLC phase. The Contractor may propose in their Technical Proposal for this RFP alternate methodologies or enhancements to the current SDLC and architecture models if the alternate or enhanced methodologies can result in the deliverables below. Prior to using any alternative or enhanced methodologies, the Contractor must receive approval from the State. Note: The repository for all of these artifacts is the State’s maintained Microsoft SharePoint and ALM. The State maintains permissions, hosting, templates, and overall operations of these repositories and tools. The Contractor is responsible for organizing and maintaining all artifacts within SharePoint and the ALM. The Contractor is also responsible for configurations of build and deployment components within the ALM.

| **Phase** | **Deliverables** |
| --- | --- |
| 1. Project Definition (Charter Development) | * Signed Project Charter * Updated MR Program Timeline * MR Scope Document, including level of effort estimates * Project Schedule * Enhancement and defect work items from the ALM updated with Business Analyst, Developer, and Tester assignments |
| 1. Requirements Definition and Analysis (Requirements Modeling) | * Updated MR Program Timeline * Updated MR Scope Document, with revised estimates * Updated Project Schedule * Requirements Document(s)   1. Update requirements in ALM * Requirements Traceability Matrix (RTM) Updates in ALM * Form Specification(s) * User Interface Specification(s) * Business Use Case(s) * Process Flow Document(s) * Security Impact Analysis (SIA) in each security-relevant deliverable (See Section 5.8, Security) |
| 1. Technical Definition and Analysis (Technical Design) | * Technical Design Document(s) (See Attachment K for examples) * Architectural Specification(s) * Updated Project Schedule * Updated Requirements Document(s), as necessary   1. Requirements and RTM Updates in ALM, as necessary * Completed Design Review Report |
| 1. Testing | * Master test plan that complies with FNS Test Plan requirements: <https://www.fns.usda.gov/apd/apd-testing-items-faqs> * Test plans for each testing phase * Documented test cases * Completion of all applicable testing cycles – System Testing, Integration Testing, End-to-End Testing, Regression Testing, Performance Testing, Security Testing, User Acceptance Testing (UAT), and Production Testing. * Updated SDLC artifacts (e.g. Requirements Document(s), Forms Specification(s), User Interface Specification(s), Business Use Case(s), Process Flow Document(s), * Fully tested system, ready for production environment * For all security defects: a final vulnerability scan reports with all High and Moderate priority defects (as defined by MARS-E 2.0 and subsequent versions) remediated (for Moderates, approved compensating controls or workarounds approved by DFR in place). The report will group defects by the categorization provided in [NIST 800-53 Rev4](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf) for the purposes of reporting compliance. See Section 5.2 for more information on vulnerability scan expectations. * Security Test Plan report (See Section 5.2.1) |
| 1. Implementation | * Maintenance Release Deployment Plan * Updated MR Project Schedule * Documented “Smoke Test” results * Operational production environment |
| 1. Post-Implementation Support (Production Support) | * Defects documented in Jazz with assigned severity and priority * “Lessons Learned” Document * Final deliverables and supporting work product documentation posted in SharePoint * New Application Scan Baseline Report, if required (See Section 5.2.1 for Security Requirements and consideration of them throughout SDLC phases. See Section 5.3.4g for Application Scan details (while conducting Application Scan is part of supporting federal requirements, it can also be part of the testing with confirming compliance with some Security Requirements determined throughout SDLC phases)) |
| 1. Defect Management | * Defect records created in Jazz * Jazz defects updated with a description of the nature and cause of the defect, as well as an assigned severity and priority, or closed out with the justification noted * Defects to be implemented within an MR * Defects to be implemented outside an MR (i.e., a non-MR implementation) * Preventative maintenance work items from Jazz * Change Request, if available * Defect Statistics Report * See Section 5.3.5 for additional information on defect management |
| 1. Change Management | * Completed and approved Change Requests * Completed and approved Change Analyses with associated Estimating Worksheets (for AS internal planning purposes) * Listing of prioritized Preventative maintenance work items from Jazz * Approved Change Requests and/or preventative maintenance changes to be implemented within an MR * Approved Change Requests and/or preventative maintenance changes to be implemented outside an MR (Non-MR implementation) |

See Attachment K for the file entitled “AS Process Overview\_SDLC\_v4.3.pdf” for the current AS SDLC.

**OV&V Contractor Checkpoints**

The OV&V Contractor will review deliverables at specific checkpoints during the SDLC process. The review at each checkpoint will consist of the following items before a sign-off can occur and the process can move forward:

* Accurate and consistent documentation of the project and SDLC artifacts
* Completion of all risk mitigations, issue resolutions, and action items
* All Severity Level 1, 2, 3 defects and all Critical, High, and Medium Priority fixed. Any residual defects have acceptable workarounds or compensations approved by DFR (see Section 5.3.2 for defect Priority Levels)

The OV&V Contractor shall be granted access to all documentation repositories. This strategy will allow the OV&V Contractor to easily access any documentation and follow changes as they are made.

* + 1. **Security Requirements by Phase**

The information below is provided to give the Contractor an understanding of the security-related activities required as part of the development of deliverables in each applicable phase of the current SDLC process. The Contractor shall perform the following key tasks/activities during each SDLC phase:

* Requirements Definition and Analysis
  + Incorporate relevant security requirements based on FSSA Privacy and Security policies and Federal security requirements, including but not limited to current MARS-E 2.0 (and subsequent versions) standard. See Attachment B, Section 12 for full list.
  + Include the Contractor’s Chief Information Security Officer (CISO) as a reviewer of each of the stated deliverables where there is a security change or impact.
  + The CISO will provide the content and final approval for a section entitled “Security Impact Analysis” which is to be added to each of the security-relevant deliverables. This impact analysis will include a risk assessment of the security changes.
* Technical Definition and Analysis (Technical Design) (See Attachment K for examples)
  + Develop the technical design and architectural specifications, which must outline all security specific components that are changing, and be risk reviewed and approved by the CISO.
  + Develop or update the Security Architecture document.
  + Determine and document any baseline configuration changes. Note that all baselines are required to be updated yearly.
  + Determine and document any new and significant changes to security functions and determine additional security controls required to mitigate risks to a level acceptable to DFR. Requires approval by the Contractor CISO.
* Construction
  + Complete software development consistent with the “General Application Security Development Standard”. The updated code is checked into the code repository.
  + Run all National Institute of Standards and Technology (NIST) RA-5 security vulnerability tools beginning in this phase to ensure all flaws and vulnerabilities are resolved throughout the remaining phases, before go-live of any artifacts to production. As part of this phase, also use NIST SI-2 techniques to support identification and triage of system flaws as well as flaw remediation.
* System Integration Test
  + Develop Security Test Plan that includes IOT Security Engagement Checklist (see below) and Federal security requirements.
* User Acceptance Test
  + Execute the full Security Test Plan and provide results throughout execution to DFR.
  + Vulnerability Scans
    - Execute the final set of vulnerability scans (outlined in the Security Test Plan) to confirm that no new security vulnerabilities have been introduced by the changes associated with the release.
    - Ensure that all High and Medium vulnerabilities (as defined by MARS-E 2.0 and subsequent versions) have been remediated and/or compensating controls have been applied with DFR approval. DFR requires that all High and Medium vulnerabilities be remediated.
    - The final set of vulnerability includes Static and Dynamic vulnerability scans of the release code base, using applicable vulnerability assessment tools.
    - Vulnerability assessments are not limited to the UAT phase and may also occur during the Construction (Build and Unit Test) and SIT phases
  + Vulnerability scans runs may be executed against the entire solution or against specific pages (and/or URLs) to ensure that any targeted vulnerabilities have been resolved and that no new vulnerabilities have been introduced
* Change Management
  + Contractor CISO to review CRs for security impacts, and a Risk Assessment must be performed

**IOT Security Engagement Checklist**

The following is the short-list of security controls that must be completed and approved before go-live of system components. IOT and DFR must be engaged early in the development phases in order to have the controls applied appropriately and effectively:

* MARS-E 2.0 SI-4(2): Ensure that all servers are integrated with the threat management SIEM solution (application-focused SIEM events may also be required depending on risk profile of the change and availability of the SIEM service).
* MARS-E 2.0 SI-7, SI-7(1): Production servers integrated with the IOT-provided File Integrity Monitoring tool, as made available by IOT.
* MARS-E 2.0 CM-8, SA-22: Updated Information Security Component Inventory including servers and software, ensuring that unsupported system components are removed, and justification of risk is documented and approved by DFR.
* MARS-E 2.0 AU-2: Ensure that logs are configured, and space is allocated for 90-days online storage.
* Backups are configured for all servers.
* IOT provided SSL certificates are applied to relevant services.
* MARS-E 2.0 RA-5: For major changes and/or for all new services, a penetration test is required.
* Ensure that DFR and FSSA Privacy & Security are aware of firewall rule updates that must be submitted to IOT for implementation. IOT owns the firewall appliance and all updates, but the Contractor is responsible for understanding the rules that are in place and supporting compliance with IOT firewall policies. Any exceptions to firewall rule standards must be justified with compensating controls clarified and realized.
* This list is subject to update or revision as deemed appropriate by the State. The Contractor’s CISO may propose updates or revisions for State approval.
  1. **Testing** 
     1. **Overview**

The objective of the overall testing effort is to verify that any AS CR or enhancement performs according to approved design specifications and requirements and from clarification resulting from defect resolution throughout testing phases. The State will not allow a production release to go live with Severity Level 1-3 defects and Critical, High, or Medium Priority defects (see Section 5.3.2 for defect Severity and Priority Levels). Additionally, as will be detailed throughout the testing phases, this severity and priority scoring is used to inform entrance and exit criteria.

The Contractor shall conduct the following testing before production for any CRs and enhancements: Unit Testing, System Testing, Integration Testing, End-to-End Testing, Regression Testing, Performance Testing, Security Testing, User Acceptance Testing (UAT), and Production Testing. Through testing efforts, the Contractor must adhere to the following:

* Test environments will be configured correctly and in alignment with anticipated functionality prior to test execution.
* Utilize effective test standards: Develop well-documented, repeatable test standards to facilitate analysis and regression testing of identified defects throughout all test phases.
* Clearly define and measure testing entry and exit criteria: Minimize the gaps and overlaps in testing by clearly defining the objectives of each test phase/cycle and measure against entry and exit criteria to determine whether those objectives are met.
* Exercise end-to-end business process lifecycles early and often: Structure testing to support execution of end-to-end business processes.
* Prioritize what will be tested and in what order: Identify the Critical, High, and/or Medium impact requirements to be tested as early as possible to provide the time needed to resolve potential issues (see Section 5.3.2 for defect Priority Levels).
* Automate testing where possible: Utilize automated testing tools to increase test execution speed and accuracy within the testing phases.
  + 1. **Testing Severity and Priority Criteria**

Each defect will be assigned a severity and priority level.

**Severity**

Severity is the major defect categorization used to guide defect/issue resolution. This field is required when a defect is submitted and is used to classify the impact of the defect on the application and the testing process. When reporting AS defects, the following severity levels are used:

|  |  |  |
| --- | --- | --- |
| **Severity Level** | **Description** | **Example** |
| 1 | System Failure. No  further processing is  possible. | Critical to solution availability, Results, Functionality, Performance, or Usability. |
| 2 | Unable to proceed with  selected function or  dependents. | Application Sub-system available, Key Component unavailable or functionally incorrect (Workaround is not available). |
| 3 | Restricted function  Capability; however,  processing can  continue. | Non-critical component unavailable or functionally incorrect; incorrect calculation results in functionally critical key fields/dates (Workaround is normally available). |
| 4 | Minor cosmetic change. | Usability errors; screen or report errors that do not materially affect quality and correctness of function, intended use or results. |

**Priority**

In addition to the Severity level, each defect is also assigned a Priority level to help prioritize the fixes for defects using the following priority codes. The Priority Codes are an indication of the importance of the function to the business.

|  |  |  |
| --- | --- | --- |
| **Priority Level** | **Description** | **Example** |
| A | Critical | Defect is imperative to the system's ability to support business functions. |
| B | High | The defect should be fixed as soon as possible. |
| C | Medium | The defect should be fixed as soon as there are no more “A” (Critical) priority defects. |
| D | Low | The defect must be fixed before the next code drop or hand over to the next level of testing. |

* + 1. **Testing Requirements**

1. Where testing requires interactions with systems other than the AS solution, the test data analysis will be conducted and test data requirements will be submitted to the respective system owners. The following list provides the data acquisition/creation approach:

* Derive test data requirements from functional and technical requirements.
* Document test data requirements and engage the State team to confirm data needs and functional accuracy.
* Where testing requires interactions with systems other than the AS solution, communicate test data requirements to system owners and their SDLC staff, as appropriate.

1. The test data used during the testing phase will comply with the following characteristics:

* The test data used during the testing will be non-production data with no Protected Health Information (PHI)/ Personally Identifiable Information (PII) or other secure data. However, the data must be sufficiently representative of production data for sufficient testing. If production data presents a defect in a higher-level environment, and testing is required to analyze and/or test the defect mitigation, then masking will be done in compliance with Federal and State requirements prior to the data being loaded in this Test environment.
* Test data received from external systems may be utilized to execute test cases when required for testing inbound data flows and data characteristics. This transactional test data will typically be utilized to complete business flows.

1. Build Verification Testing (Smoke Testing) is comprised of a non-exhaustive set of tests that aim to ensure that the most important functions work. The result of this testing is used to decide if a build is stable enough to proceed with further testing. The Contractor shall conduct smoke testing for each testing phase prior to the start of the testing activities and after each code release into that phase’s Testing environments to confirm the environment’s and component’s readiness. Smoke Testing is conducted manually and with the automated tools.
2. The following criteria will be met before a Testing phase can begin:

* Design for scope to be tested is complete and approved by the State.
* Development of components is completed for the scope to be tested prior to test execution.
* Preceding testing phases are complete for the scope to be tested prior to test execution.
* Vendor partners, as appropriate, are available for the phase’s Testing.
* The environment is configured correctly and in alignment with anticipated functionality prior to test execution. The environment has been smoke tested.
* The schedule and scope of testing to be executed has been defined.
* All testing tools are installed and configured for developers.
* Access permissions have been requested and acquired for any users needing such privileges.

1. The following criteria must be met before a Testing Phase can be considered complete:

* Achievement of 100% Execution with 100% Passed
* Any defect and risks identified during Testing have been identified with mitigation strategies.
* Defects with Severity 1 or 2 are resolved and associated functionality is working correctly. Defects with Priority A or B are resolved and associated functionality is working correctly.
* Defects with severity 3 have documented workarounds approved by the State.
  + 1. **Required Types of Testing**

The Contractor is required to conduct all of the following phases of testing for each CR unless otherwise approved by the State.

1. **Unit Testing.** Unit testing is performed on each isolated unit of an AS solution component prior to integrating them to validate that each unit is working as expected. Each unit test case is scheduled and executed by a developer who developed the unit and has knowledge of the component’s functionality. Scenarios and cases are derived from requirement and design documentation. These test scenarios and cases created by developers are reviewed by the State for approval. Developers are encouraged to use, where optimal, automated regression Unit Testing tools and approach to augment their Unit Testing validation efforts. It is anticipated that “stubbing out” of interfaces may be a strategy employed for System Testing.
2. **System Testing.** System testing is the process of validating the AS solution component against requirements and design specifications. System Testing scenarios and cases will focus on validating non-functional requirements as well, including Section 508 Compliance, usability, performance, and compliance with security regulations and expectations. It is anticipated that “stubbing out” of interfaces may be a strategy employed for System Testing.
3. **Integration Testing.** Integration Testing validates that all related system and functional components maintain data integrity and can operate in coordination with other sub-systems in the same environment. The testing process confirms that all functional components are integrated successfully and provides expected results. It is anticipated that interfaces would not be “stubbed out” for this testing, unless it is unavoidable (e.g., interface partner does not have a test environment).
4. **End-to-End Testing.** End-to-End Testing will validate the integration and system transaction flows in the AS solution, while also factoring in interface partners and their systems as appropriate. End-to-End test scenarios and test cases will be created by the Contractor test team and reviewed by the State for approval prior to execution. Similar to Integration Testing, it is anticipated that interfaces would not be “stubbed out” for this testing.
5. **Regression Testing.** The Contractor testing team will create and execute Regression Testing scenarios and cases, with the State’s approval, for AS solution components along with interface partner components to confirm that functionality does not regress across components based on approved requirements and design. Additionally, the Contractor and the UAT team, as appropriate, will conduct Regression Testing of “old” test scenarios and test cases when defect fixes or CRs are tested so that no related functionality fails following defect fix or CR development efforts.

The test cases for Regression Testing will be identified during test design and execution primarily in the System Testing, Integration Testing, and UAT phases. The regression test suite will be maintained and updated after each major release to System Test Phase.

Both manual and automated Regression Testing is encouraged to streamline and support quality SDLC.

1. **Performance Testing**

The focus of Performance Testing includes validating: the AS solution’s behavior under both normal conditions and peak load conditions, that inbound services can handle the anticipated normal conditions and peak load conditions for incoming requests, that outbound services can be generated to critical partners for anticipated normal conditions and peak load conditions, and that the batch cycles can complete within the batch window.

In addition to the exit criteria in Section 5.3.3, the AS production environment will be load tested for performance to measure whether it can accomplish, at a minimum, M&O SLA performance (see Section 12.2.1 for SLAs).

Automated Performance Testing is encouraged. The State owns Rational Performance Tester (RPT) licensure that is available for the Contractor’s use.

1. **Security Testing**

Security testing is conducted using the methodologies cited by MARS-E 2.0 (and subsequent versions) and FSSA Policies. The testing will confirm that implemented security and privacy safeguards are in compliance with Federal and State security requirements as they pertain to MARS-E 2.0 (and subsequent versions), HIPAA requirements, and FSSA Policy. Please see Section 5.8 and Section 10.1 for the full description of contractual security standards.

The entry criteria for Security Testing are:

* Design completion: System Requirements, Non-Functional Requirements, Security Requirements, Preliminary System Design, Detailed System Design, and technical artifacts are finalized and approved.
* Testing readiness
  + Test cases for Security & Privacy Control Testing are completed and are reviewed by the Contractor and State security teams.
  + Test cases for Logging & Monitoring are completed and are reviewed by the Contractor and State security teams.
  + Approach for Vulnerability Scanning is approved by the State.
  + Approach for Application Scanning is approved by the State.
* Testing tools are made available and configured.
* Test environments are made available and have been successfully Smoke Tested by the Contractor.
* Note: Enterprise wide Infrastructure vulnerability and functional security testing (e.g., servers and network) will be the responsibility of the State. The AS solution-related vulnerability and security testing as well as Application Scanning will be conducted by the Contractor. The State may conduct vulnerability assessment activities, either via State resources or via third party assessor. Regardless, they may employ vulnerability assessment activities, including vulnerability scans and Application Scans. The Contractor must support the State and/or third party assessor in ensuring environment and application availability for these activities. The Contractor must also address the findings and defects, as applicable, generated from these activities.

The exit criteria for Security Testing are:

* Testing completion
  + Vulnerability Scanning activities have been completed.
  + Application Scanning activities have been completed.
  + Planned Test Cases for Security & Privacy Control Testing have been executed.
  + Planned Test Cases for Logging & Monitoring have been executed.
  + Vulnerability Scanning results have been shared and approved by the State.
  + Application Scanning activities have been shared and approved by the State.
  + Test results for Security & Privacy Test Cases have been shared and approved by the State.
  + Test results for Logging & Monitoring Test Cases have been shared and approved by the State.
  + Go/No-Go meeting is conducted with State and the Contractor to review the test results.
* Risk
  + Mitigation strategy has been identified for the risks identified during the security testing activities (i.e., Vulnerability Scanning, Application Scanning, Security & Privacy Controls Testing, and Logging & Monitoring).
  + Residual risk expected as employing this strategy.
* Defects
  + Defects with Severity 1 or 2, or defects with Priority A or B identified during security testing (i.e., Vulnerability Scanning, Application Scanning, Security & Privacy Controls Testing, and Logging & Monitoring) are resolved.
* Note: Go/No-go meeting(s) will be conducted with the State and the Contractor to review security test results.
  + Unresolved defects with Severity 1 or 2, or unresolved defects with Priority A or B may result in a No-go decision for release.
  + The decision to migrate the secure code into a pre-production environment will be made by the State, FSSA Privacy & Security, the Contractor, and other key project stakeholders.

1. **User Acceptance Testing (UAT)**

The UAT phase confirms that AS solution releases are production ready. The purpose of this testing is to evaluate the solution’s compliance with the approved requirements and design. UAT is performed only after Severity 1 and 2, and Priority A or B defects have been resolved in lower level testing.

The Contractor shall support the State throughout all UAT tasks. The major tasks are outlined below.

| Test Phase | Task | Description | Contractor Responsibility | State Responsibility |
| --- | --- | --- | --- | --- |
| Test Analysis | Requirements Review | Identify and review requirements and CRs | Identify applicable artifacts for State | Review in prep for UAT |
| Test Analysis | Design Documentation Review | Identify and review design documents that implement the requirements. | Identify applicable artifacts for State | Review in prep for UAT |
| Test Analysis | Traceability Review | Identify and review the requirement traceability in order to identify any potential gaps in coverage that need to be addressed during UAT. | Identify applicable artifacts for State | Review in prep for UAT |
| Test Planning | Metrics Reporting Development | Develop, document, and communicate the metrics to be reported during UAT and the mechanism for communication of those metrics. | Support State in clarifying this mechanism and reporting | Be prepared to provide the requested metrics and reporting for UAT |
| Test Design | Workflow Mapping | In conjunction with State SMEs, identify and document the high-level workflows implemented by the system, including End-to-End workflows incorporating interfaces, including those with interface partners. | Identify applicable items. | Review and meet with Contractor and State SMEs, as applicable, to work through this effort. |
| Test Design | Test Case/Test Script Development | Identify, prioritize, and document test case scenarios and the positive, negative, and alternate flows necessary to validate all requirements and design specifications. | Address State concerns or questions. | State is responsible |
| Test Preparation | Test Data Development | Define and create the test data required to successfully execute documented test case scenarios. | Support the State in mocking up any interface files and/or other items that the State cannot interact with directly (e.g., database table mock-ups if applicable). Support the State in determining the overarching rules for test data (e.g., conventions and standards). | Work with Contractor on the overarching rules for test data (e.g., conventions and standards).  Create scenarios that include clear test data and mock-up data in the test environment, as applicable. |
| Test Preparation | Test Case Review | In conjunction with State SMEs, review test case scenarios to ensure that all necessary flows have been incorporated into test scripts and that all requirements are covered. | Address State concerns or questions. | State is responsible |
| Test Preparation | Test Script Validation | Dry run of test scripts on UAT environment. | Address State concerns or questions. | State is responsible |
| Test Execution | Test Case Execution | Execute each test case scenario and document execution results, including defects. | Address State concerns or questions. | State is responsible |
| Test Execution | Execution Results and Defect Reporting | Develop, document, and communicate the results of test case execution, including defect status, through standardized reports. | Generate the reports based on the data the State has provided in their UAT efforts. | Provide the data for the reports. |
| Defect Resolution | Defect Management | Triage and fix defects for retest. (See Section 5.3.5 for details.) May repeat this Phase and Test Execution Phase as applicable. | Facilitate triage discussions with the UAT team, and fix applicable defects. Document in the ALM the results of triage and any next steps on the defect, up through State retest. | Attend and provided feedback in triage discussions to support the Contractor through defect management efforts. Retest defects and/or defect fixes as applicable. |
| Test Closeout | Test Closeout | Develop, document, and communicate test closeout results upon completion of UAT. | Contractor to provide reporting based on UAT team-provided data. | Provide data to support this reporting. |
| Test Closeout | UAT Sign-off | Upon successful completion of UAT, provide a recommendation to the State pertaining to the AS solution component’s readiness for production deployment. | Contractor to provide reporting based on UAT team-provided data. | Provide data to support this reporting. |

As opposed to the earlier phases of testing (e.g., System Testing and Integration Testing), Smoke Testing for this phase is handled by both the Contractor and the UAT team. This ensures that the Contractor can support the build process while UAT can signal a build failure as soon as possible for the testing that they had anticipated to undertake. Both manual and automated smoke testing is encouraged, to validate a build prior to in-depth UAT activity.

**The Contractor’s test plan and project schedule must allocate enough time for comprehensive UAT for all applicable functionality including the opportunity for regression UAT and retests of defect fixes.**

The entry criteria for UAT are:

* Design Completion: System requirements, preliminary and detailed design documents shall be finalized and approved by the State.
* Testing Readiness
  + Integration Testing is complete; defects with Severity 1 or 2 are resolved and associated functionality is working correctly. Defects with Priority A or B are resolved and associated functionality is working correctly.
  + Defects with Severity 3 have documented workarounds approved by the State.
  + Go/No-go decision has been made by the key project stakeholders on proceeding with UAT for the scope to be tested.
  + Test cases are documented with test data aligned with the Test Cases.
* Interface Partner Readiness: Integration Testing for vendor partner systems’ components is complete and interface testing is completed with functionality is available for UAT.
* Testing tools are made available and configured.
* The UAT environment is available, configured, and has been successfully Smoke Tested.
* During the execution of Test Cases, the Contractor team will notify the UAT team, in writing, of any change in design and/or defects introduced.

The exit criteria for UAT are:

* Testing Completion
  + Planned test cases for UAT have 100% been executed and retested, as applicable.
  + Go/No-Go meeting is conducted with State and testing stakeholders to review UAT results.
* Risk
  + Mitigation strategy has been identified for the risks compiled within the UAT phase.
  + Residual risk is identified for each phase of the mitigation strategy, as applicable
* Defects
  + All Defects with severity 1 or 2 are resolved and associated functionality is working correctly. Defects with Priority A or B are resolved, and associated functionality is working correctly.
  + Defects with severity 3 have documented workarounds approved by the State.

1. **Production Testing**

The purpose of Production Testing is to Smoke Test with identified End User and SME staff as appropriate to ensure that the Production build is working as anticipated. With successful Production Testing, the build deployment into the Production environment can be signaled as appropriate for Production use.

The entry criteria include:

* A fully documented Implementation Plan approved by the State that includes rollback criteria and plan to support critical issue mitigation.
  + Scenarios and owners of Production Test Scenarios/Cases documented in Implementation Plan.
* Go vote from DFR to deploy a production build.
  + The Release Management Plan indicates all the representatives who contribute to Go recommendations for DFR.
* All lower level testing is complete with all defects with Severity 1 or 2 resolved and associated functionality working correctly. Defects with Priority A or B are resolved and associated functionality is working correctly. Defects with Severity 3 have documented workarounds approved by the State.

The exit criteria include:

* The Implementation Plan is completed for the Production build deployment, including all the Production Testing that was scoped in the plan.
* Defects with Severity 1 or 2 are resolved and associated functionality is working correctly. Defects with Priority A or B are resolved and associated functionality is working correctly.
* Defects with Severity 3 have documented workarounds approved by the State.
  + 1. **Defect Management**

Defects are discrepancies between the documented expected system behavior and the actual system behavior encountered during testing. The discovery of a defect will result in either documentation update(s) and/or development resolution(s), and upon resolution, the Contractor, the State testing team, and/or interface partners will be engaged to verify the fixes. Defect management requirements are highlighted in this section, but the full details of defect management will be developed in the Defect Management Plan, which will be finalized with the Contractor upon project initiation.

When a tester finds a defect, the tester will enter the defect into the ALM and assign the Severity and Priority level. The lifecycle of a defect is detailed below:

1. **New** – A defect is new when it is first created.
2. **Triaged** – A defect is being analyzed by the Contractor.
3. **Assigned** – The defect is triaged and assigned to the Contractor.
4. **Development in Progress** – A valid defect is assigned to the Contractor and the developer(s) begin(s) working on it.
5. **Development Complete** - A fix for the defect is complete.
6. **Build Deployed** – A fix for the defect is complete and ready for deployment to the appropriate test environment.
7. **Ready For Test** – A defect has been deployed and is ready for the Contractor test team, the UAT team, and the interface partner team to retest, as appropriate, the defect fix to validate that the system operates per design.
8. **Closed** – A defect has been retested successfully and closed.
9. **Cancelled** - A defect that is invalid or is a duplicate can be Cancelled.

The defects can follow the following alternate paths:

1. **Withdrawn** – A defect that is invalid or duplicate can be withdrawn.
2. **Rejected Defect** – A defect with an unsuccessful fix validated by the testing team (Contractor team, UAT team, and/or interface partner) will be rejected for the Contractor to readdress the defect fix.
3. **Return to Testing** – A defect can be returned to testing team (Contractor test team and/or UAT team) if the information in the defect is not adequate and the developer(s) seek(s) more information.

**Defect Management Meetings:** At defect management meetings, the **Priority** and **Severity** of defects will be reviewed. For the defects where any clarification is required, the tester and/or SMEs (from State and the Contractor) will also be a part of the meeting. DFR leadership will be kept informed on defect status through defect reports and regular management and testing meetings.

**UAT Defect Remediation Schedule:** Defects identified during UAT testing must be fixed within the following timeframes:

* Severity Level 1 or Priority Level A defects must be fixed within one (1) business day
* Severity 2 or Priority Level B defects must be fixed within two (2) business days
* The State and the Contractor can agree upon criteria for resolution time frames for all other Severity Level and Priority Level defects

**Post Go-Live Defect Escalation:** The escalation timeframe for defects post go-live by Severity and Priority is listed below:

| Defect Type | Post Go Live Escalation Time Frame |
| --- | --- |
| Severity Level 1 or Priority Level A | One (1) Hour |
| Severity Level 2 or Priority Level B | One (1) Day |
| Severity Level 3 or Priority Level C | Three (3) Days |
| Severity Level 4 or Priority Level D | One (1) Week |

**Defect Logging Guidelines:** Defects should be resolved in the most expeditious manner. They should be well-written and minimize the need for clarifications requested by the State Test Lead and other State team members, interface partners, and Federal partners. Where possible, the tester should include screen shots of the error, videos of the test process that resulted in the subject defect, or similar information that will allow the State to make a full and complete assessment of the defect and thereby design and develop a complete fix.

The content should have the following information:

* A descriptive name (e.g., “Unable to open account”)
* A full description of the defect (e.g., “When creating a new account, error message 101 is returned when submitting the record”)
* Clear steps to reproduce the defect / a breakdown of the test steps leading to the detection of the defect
* Test Case name and number
* Test Script name and number
* Expected Result
* Actual Result
* Screen shot(s) when applicable
* Screen URL(s) when applicable
* SQL query statement(s) when applicable

In the “Steps to Reproduce”, anyone with basic knowledge of the system should have enough detail to adequately reproduce the defect.

* 1. **Artifact Management**

The Contractor is expected to maintain existing artifacts for Program/Project Management, Requirements and Technical Definition and Analysis, Design, Construction, Testing, other SDLC processes, and Helpdesk. Additionally, the Contractor must update these artifacts and generate new artifacts, as applicable, throughout the SDLC process. The State will make available an ALM tool, as well as document repository for these purposes (see Section 2.6 on the ALM and Microsoft SharePoint for the document repository).

* 1. **SDLC Quality Management**

While conducting SDLC processes, the Contractor must ensure that it has an ongoing SDLC Quality Management process. This will take the form of information sharing, regular meetings to review quality data feedback, lessons learned with action plans developed following each MR, and the establishment of common continual improvement goals and objectives. As a part of SDLC Quality Management responsibilities, the Contractor shall:

* 1. Develop quality assurance (QA) functions to regularly monitor performance and compliance of each business process managed by the Contractor
     1. QA should be conducted against all SDLC phases
  2. Work with the OV&V vendor on quality assurance as directed by the State
  3. Develop a Quality Management Plan (to be approved by the State) that focuses on being proactive and preventing problems rather than allowing problems to occur, and on ensuring that work products and deliverables meet business objectives, end-user expectations, and defined requirements
  4. Provide information about the impact of a solution component deficiency, proposed an action plan, and describe any appropriate workaround to appropriate State stakeholders
  5. Provide a well-researched and clearly explained root-cause analysis for any issue including, but not limited to, a description of the problem, action plan to be taken, and measures that will be taken to prevent such a problem in the future. The written root-cause analysis shall be provided within seven (7) calendar days of the resolution of the situation addressed by the root-cause analysis. Document this information within the ALM where the defect or defects related to the incident are logged
  6. Include information about QA status and improvement in MR reporting
  7. Report results of any State-required audit within thirty (30) calendar days of the audit, providing the Contractor's detailed response including any actions to be taken by the Contractor to effectively correct any negative findings
  8. Implement Corrective Action Plans (CAPs) as needed to correct quality concerns
  9. Complete all necessary corrective measures within ninety (90) calendar days of receipt of the audit findings or on a schedule agreed to by the State
  10. Provide a report within ninety (90) calendar days of receipt of the audit or on a schedule agreed to by the State detailing the corrective measures undertaken to respond to audit findings
  11. **Technical Services** 
      1. **Software/Hardware Management**

While IOT is responsible for managing server hosting, DFR, as the owner of E&E and E&T systems, is expected to maintain an understanding of the AS solution components and how they use the underlying infrastructure. Because of this framework, the Contractor must support DFR by maintaining a detailed listing of all hardware and software supporting AS solution components. This detailed listing includes all AS solution components they support. It must include the components’ types, versions, descriptions of what they provide, their interrelationship to other software/hardware components, and other related information. This information will be critical for the Contractor to have as a basis for Configuration Management, Change Management, Architecture, BCP/DR planning, Security Management (Section 5.8), and incident management (Section 5.6.6).

See Section 4 for details on these expectations within the SDLC.

The Contractor is expected to maintain existing Software/Hardware Management artifacts. Additionally, they must update these artifacts and generate new artifacts, as applicable, throughout the term of the contract.

* + 1. **Infrastructure Management**

The Contractor shall work with IOT to manage overall server strategy, maintenance, and monitoring for the AS solution. While IOT manages the infrastructure, including all servers and the tools to monitor them, they will make CPU, memory, hard drive utilization, outage information, and security incident information available to DFR and the Contractor to monitor or address, as applicable. The Contractor must work with DFR and IOT on maintaining infrastructure architecture and tool set (the State is responsible for licensure on servers) for all applicable non-production and production users. The Contractor must support current and forecasted utilization “counting” of licensure in non-production and production environments. While DFR and IOT manage the licensure agreements, the Contractor supports the State in ensuring that DFR maintains licensure agreements with applicable parties. The Contractor must plan and execute tasks required to ensure AS solution components stay relevant and useable. This support includes resolution of functional issues, application of patches, preventative maintenance, planning/execution of upgrades, and regular performance monitoring and performance reporting. Conduct relevant SDLC procedures as necessary. At least on an annual basis, the Contractor shall communicate to the State any available information on the product roadmap, planned upgrades, and enhancements, and seek State input when necessary.

* + 1. **Application Lifecycle Management (ALM)**

The State has ALM solutions with IBM Rational Jazz, Atlassian Jira, and various Open Source tools. While the State maintains these platforms, overall configuration, and role-based access approval, the Contractor is expected to maintain code, requirements, design artifacts, testing artifacts, and build management/configuration within these tools

The incumbent vendor is expected to, prior to current contract expiration, provide the most recent and up-to-date versions of requirements, design artifacts, architecture diagrams, business process models (BPMs), security diagrams, build processes/configurations, infrastructure listings/diagrams, and other SDLC artifacts.

* + 1. **Database Support**

The Contractor must provide Database Analyst (DBA) support with extensive knowledge in multiple database technologies and best practices (see Section 2.6 for the different database technologies being used).

See Section 4 above for details on these expectations within the SDLC.

The Contractor is expected to maintain existing database-associated artifacts. Additionally, they must update these artifacts and generate new artifacts, as applicable, throughout the SDLC process.

* + - 1. **Database - Conceptual Data Model (CDM)**

The CDM provides a mechanism to bridge the gap between SMEs and IT architects and designers. The model depicts the major business information objects (subjects/entities) in their relationships to each other using business terminology. The CDM has the following associated data: Entities, Relationships, Definitions, Domains, Related Standards, and Entity-Relationship Diagrams.

As a part of database support, the Contractor shall manage the conceptual data model, standards, entities, relationships, definitions, domains, and entity-relationship diagrams.

Details on CDM Federal requirements are provided under MITA and MEET.

* + - 1. **Database - Logical Data Model (LDM)**

The LDM provides policy and procedure for the establishment and maintenance of the following: physical data model, the business model, and the reengineering of business processes. The LDM has the following associated data: Entities, Relationships, Definitions, Domains, Related Standards, and Entity-Relationship Diagrams.

The Contractor shall manage the LDM, including the following responsibilities:

1. Manage the logical and physical data model, standards, entities, relationships, definitions, domains, and entity-relationship diagrams.
2. Manage the established business model standards.

Details on LDM Federal requirements are provided under MITA and MEET.

* + - 1. **Database - Data Standards**

The data standards provide a syntactic and semantic understanding of the State’s data and information. As a part of data standards, the Contractor shall:

1. Manage the metadata development and maintenance approach, metadata, and standards.
2. Manage the data standards (specify how data should be formatted or structured).
3. Manage the structure data standards. The structure data standards and vocabulary data standards include the following: Title, Category, Objective, Source, Type, Version, Status, Applicability, References, relationships to other standards, and Key Terms.
4. Manage the vocabulary data standards (i.e., specify the meaning of the data and its use).
5. Publish and maintain the metadata standards, data standards, structure data standards, and vocabulary standards.

Details on Federal requirements for Data Standards are provided under MITA and MEET.

* + 1. **Application Monitoring**

The Contractor must monitor all AS solution components to ensure that they are available per State requirements and in alignment with meeting and exceeding applicable SLAs (Section 12). While IOT monitors infrastructure components that they host and can make information available to the Contractor from the mechanisms they use to monitor (e.g., Security Operations Center (SOC) and Network Operations Center (NOC) tools that monitor CPU, memory, hard drive utilization, malware issues, Data Loss Prevention (DLP), network traffic, and server logs), the Contractor is responsible for monitoring all AS solution components. This monitoring supports troubleshooting, security incident management (see Section 5.8, Section 10.1, and Attachment B, Section 12), and Helpdesk Support (see below). Additionally, information from Application Monitoring demonstrates areas of risk where the Contractor must indicate recommendations on architecture or software/hardware adjustments that could be made to minimize operational risk.

See Section 4 above for details on these expectations within the SDLC.

The Contractor is expected to maintain existing Application Monitoring artifacts. Additionally, they must update these artifacts and generate new artifacts, as applicable, throughout the SDLC process.

* + 1. **Incident Management and Helpdesk Support**
       1. **Helpdesk Tickets**

The Contractor must support the triage and resolution, as applicable, for all Helpdesk tickets. There are three types of AS Helpdesk tickets – Internal, External, and Agency Portal-specific.

The incumbent contractor currently staffs two employees part time on reviewing, responding to, and routing internal tickets, external tickets, and Agency-Portal tickets. The historical volumes of tickets have been shared below for informational purposes only. Short-term increases in the volume of tickets directed to the Contractor are expected with new releases that change the interface or functionality, and with the rollout of IEDSS. As part of their planning and staffing strategy, the Contractor must be prepared to handle these increases effectively.

**Internal and External Tickets.** Internal and external tickets are routed to the Contractor by either IOT or DFR’s service desk vendor, working on behalf of IOT. These two entities are the Tier 1 team for the Internal tickets. The tickets can originate from phone calls or via website. Internal and external tickets cover all AS solution components except for the Agency Portal.

Internal Tickets

* + **Submitted By:** DFR Central Office Staff, DST Central Office Staff, E&E Workers, IMPACT Workers, OHA Workers, partner systems, and IOT
  + **Routed To:** Appropriate AS staff to resolve AS solution issues, IOT Helpdesk and/or IOT Helpdesk designee to resolve (infrastructure issues), ICES Policy Answer Line (PAL) to resolve (casework policy issues or ICES issues), or IEDSS to resolve (IEDSS issue or defect)
  + Analysis of July 2017 to June 2018 ticket data shows an average of 1,320 internal tickets are received by DFR’s service desk vendor on a monthly basis. The majority of tickets are resolved by IOT and DFR’s service desk vendor. They will route to the Contractor any AS-specific tickets (i.e., those pertaining to one of the AS components) that they are unable to address. Please see Attachment K for excerpts from the DFR Helpdesk vendor’s process document.

External Tickets

* + **Submitted By:** Clients, Authorized Representatives (ARs), or Agencies working in some capacity on behalf of clients (i.e., Agency Portal users)
  + **Routed To:** Appropriate AS staff to resolve AS solution issues (e.g., user changes): see <https://www.in.gov/fssa/dfr/4323.htm>.
  + Analysis of July 2017 to June 2018 ticket data shows an average of 2,430 external tickets are received by DFR’s service desk vendor on a monthly basis. Account access issues typically total 70%+ of the tickets. The vast majority of external tickets are resolved by the customer service agent, typical through the use of the Known Error Database (KEDB). Of the remaining external tickets, IOT and DFR’s service desk vendor will route to the Contractor any AS-specific tickets that they are unable to address.

**Agency Portal -Specific Tickets.** Agency Portal-specific tickets are received directly by the Contractor. Currently, on average 10-15 tickets are received by the incumbent AS vendor per week. The Agency Portal is fully administered by the Contractor, including the role-based access provided to agencies. A process is in place that includes forms for agencies to complete and captures contact information for agencies and other related information to support this process. See <https://www.in.gov/fssa/dfr/4323.htm> for more information.

* + - 1. **Incident Resolution**

Incidents are created from tickets and one incident can be linked to multiple tickets if they pertain to the same issue. All incidents will be tracked through DFR’s service desk vendor Helpdesk, with the following priority levels:

|  |  |
| --- | --- |
| **Priority Level** | **Incident Description** |
| 1 | A critical in-scope system function is unavailable or severely degraded, causing a significant impact on the processing operations of end users. |
| 2 | A system function that is not critical to processing operations is unavailable or severely degraded, with no reasonable alternative or bypass available to a Service Recipient. |
| 3 | A system is degraded or is unable to be fully used by Service Recipient personnel. |
| 4 | A problem causes a minor inconvenience for Service Recipient personnel but does not prevent system usage. |

Prompt resolution is important to DFR. Agency portal password resets are resolved on the initial call. For all other calls, the Contractor will adhere to the following incident resolution times based on priority levels:

|  |  |
| --- | --- |
| **Priority Level** | **Incident Resolution Timeframe** |
| 1 | Two (2) hours |
| 2 | 24 hours; escalate to Priority Level 1 after 24 hours |
| 3 | Three (3) Business Days; escalate to Priority Level 2 after Three (3) Business Day |
| 4 | Five (5) Business Days; escalate to Priority Level 3 after Five (5) Business Days |

For incidents related to tickets from IOT or the DFR service desk vendor, the incidents will be tracked in vFire, maintained by IOT. For incidents related to the Agency portal, incidents are entered into Rational.

* + - 1. **Helpdesk Staff Responsibilities**

As a part of Helpdesk Management, the Contractor shall:

1. Provide Helpdesk Management services for tickets sent to the appropriate Contractor or partner staff. Provide the subject matter expertise for all levels of support. Provide appropriate, accurate, courteous, efficient, timely and proactive responses to inquiries. Service requests can be submitted via email or phone.
2. Provide on-site qualified incident support from 8:00 AM to 6:00 PM Eastern Time, Monday through Friday, except for State holidays. Incident support shall adhere to the timeframes listed in Section 5.6.6 based upon the request’s function type and severity code for problems that cannot be resolved via telephone.
3. Provide after-hours support (defined as from 6:01 PM to 7:59 AM Eastern Time Mondays to Fridays, as well as full day (24 hours a day) weekends and State holidays) will be provided via phone and email. Required response times for incidents reported outside of normal business hours will be determined based on the severity of the incident (see Section 5.6.6).
4. Acknowledge tickets routed to the Contractor by DFR’s service desk vendor promptly
5. Perform a triage function for all inquiries received at the dedicated e-mail address and phone line(s). For those inquiries that are determined to be outside of the scope for the Contractor and/or should be handled by State staff, forward to the designated State staff within one (1) business day.
6. Provide adequate training and access to information to Contractor staff to facilitate timely and accurate responses to inquiries.
7. Coordinate responses by following Helpdesk triage and escalation workflows that address proper handling of requests.
8. Respond to and resolve all tickets by the required response time and resolution times listed in Section 5.6.6.
9. If any incidents are identified as defects, the Contractor shall follow the defect management processes described in Section 5.3.5.
   * + 1. **Incident Management**

The Contractor shall properly plan and conduct services to minimize the occurrence of incidents and/or problems with the solution components and service delivery. If incidents and/or problems arise, the Contractor shall work with the State to resolve issues in a timely manner based on the severity/priority levels of the State.

* + 1. **Access Management**

The Contractor shall assist in the definition of user roles and security configurations, specifically the creation of new roles and monitoring of user access rights in relation to internal requirements. The Contractor shall manage credentials for non-production environments and security profiles for users authorized by the State, including other contractors, to have access to AS solution components and service operations. The Contractor shall support the creation of role-based security for production environments.

* 1. **Business and Operations Reporting**

The Contractor shall be required to support reporting as needed for their respective scope. See Section 4 above for details on these expectations within the SDLC.

The Contractor is expected to maintain existing reporting artifacts. Additionally, they must update these artifacts and generate new artifacts, as applicable, throughout the SDLC process.

As part of the reporting responsibilities, the Contractor shall:

1. Maintain existing reports and data extracts
   * Via Informatica, data extracts will be provided to the State’s Enterprise Data Warehouse (EDW) for the Benefits Portal, the Agency Portal, IMPACT, and the I3/IVR. The Contractor shall explain the data dictionary, the business and technical requirements pertinent to the data provided, and any modifications to this data or applicable business/technical requirements.
   * Per current requirements and design, reports needed for the Benefits Portal, Agency Portal, IMPACT, and the I3/IVR will be created by the Contractor’s reports team and made available in the EDW instance of Cognos.
   * For the IMPACT system, DFR workers (IMPACT and Eligibility & Enrollment) staff must have access to applicable ports within this system via Birt.
2. Develop, test, implement, and manage new recurring reports in a timely and accurate way in accordance with the SDLC. Develop ad hoc reports when requested.
3. Adhere to State, Federal, or business area-defined format and distribution methodology.
4. Ensure that report requests are documented and validate that the delivered report meets the requester’s requirements for content, format, quality, and timeliness.
5. Notify the requester when report timeliness or quality standards cannot be met.
6. Store production reports based on State’s existing protocol.
7. Provide historic reports and extracts to the EDW in accordance with State, Federal, and business area retention schedules.
8. Revise existing measures, reports, and extracts when requested.
9. Maintain detailed documentation for reporting/extract logic and design.

**Data Analytics**

AS solution components have analytic capabilities that allow for quantitative and qualitative analysis of data for DFR. As part of data analytics responsibilities, the Contractor shall:

1. Manage the development and maintenance of the data analytic capabilities currently facilitated within AS solution components.
2. Maintain analytic capabilities that include, but are not limited to the following: data summarization, data comparison, forecasting, trending, and statistical analysis.
3. Conduct modeling and analysis activities to manipulate and review what-if scenarios, identify impact of potential changes, and analyze potential program additions, modification, or deletions for fiscal impact.
4. Manage required program monitoring, provide quality and management reports per business area need, and support mechanisms that will track activity and effectiveness at all levels of monitoring.

**Data Presentation**

The Contractor shall support Data Presentation, which includes the following responsibilities:

1. Maintain the methodology for the development and maintenance of the data visualization and presentation capabilities.
2. Support data presentation that includes but is not limited to: dashboarding and the ability to support a variety of formats and output options, such as Word, Excel, HTML, or PDF.

**Recurring Reports**

Per existing requirements and design, several recurring reports are made available to the business for the Benefits Portal (~20 reports), the Agency Portal (~5 reports), IMPACT (~31 reports), and the I3/IVR (~5 reports).

**Ad Hoc Reports**

Deadlines for ad hoc reports shall be determined by the State according to a scale of urgency.

* Type 1: 24 business hours turnaround time
* Type 2: Two (2) business days turnaround time
* Type 3: Five (5) business days turnaround time

Examples of ad hoc reports are reports driven by questions from DFR regarding number of online or paper applications, or numbers of E&T recipients in compliance with Applicant Job Search (AJS) requirements during particular time periods.

**Data Extracts**

Per existing requirements and design, data extracts from AS solution components are provided via Informatica to the State’s EDW. Contractor staff must be familiar with using Informatica for this purpose. The Contractor must work with the EDW vendor to maintain data extracts.

* 1. **AS Solution Security**

See Section 4 above for details on these expectations within the SDLC. See Attachment B, Section 12 on contractual obligations for this scope.

The Contractor is expected to maintain existing database-associated artifacts. Additionally, they must update these artifacts and generate new artifacts, as applicable, throughout the SDLC process.

**Security Monitoring**

The Contractor shall conduct security monitoring activities to ensure full compliance with MARS-E 2.0 and its subsequent versions. To facilitate this, the Contractor must develop and implement a Security Monitoring function to control physical and logical security (centrally and remotely), access, and auditing. A Security Monitoring Plan must be developed that includes, but is not limited to:

* Mechanisms for the implementation, monitoring, and maintaining of physical and logical security controls
* Logging of all security events
* Mechanisms for taking corrective action for security violations
* Periodic testing of security plans
* Reporting on security violations/deviations from the plan

**Federal Compliance Status Reporting**

The Contractor shall support the State with meeting MARS-E 2.0 (and subsequent versions) requirements related to federal compliance status reporting including, but not limited to, quarterly Plan of Action and Milestones (POA&M) meetings, annual System Security Plan (SSP) updates, and supporting third party assessors by making artifacts, data, SDLC resources for interview, and other related information available.

**Security Impact Analysis (SIA):**  The Contractor will conduct SIAs in compliance with CM-4 of NIST 800-53 (Rev. 4). This activity includes CM-4(1) (Separate Test Environments) and CM-4(2) (Verification of Security Functions).

# **Maintenance and Operations (M&O) Workstreams**

There are eight (8) M&O workstreams in this Contract. When IEDSS is rolled out:

* The Time-limited workstreams will not be needed and the Contractor will cease billing the State the monthly fees for those workstreams. Any short-term transitional activities (support for archival, decommission and conversion to any new components) will be billed at actual hourly rates used, with prior approval by the State.
* The State and Contractor will review staffing levels for each M&O workstream on a quarterly basis to determine if staffing levels need to be changed to reflect a change in the scope of M&O activities. All changes to M&O monthly fees for each workstream must be approved by the State before going into effect.

The following subsections provide further detail on each M&O workstream:

* Interface partners and user information is provided by workstream as the Contractor must work with these parties during each workstream.
* Please see Section 2.1 for additional background for each workstream.
* Please see Section 2.5 for user count information for each workstream (except for Workstream 5 (CDMS M&O)).
* Please see Section 2.6 for technology toolset information for each workstream
* Sections 4 and 5 detail the required Contractor services and support that apply to all workstreams.
  1. **Workstream 1 - Benefits Portal M&O**

The Benefits Portal (<https://fssabenefits.in.gov/>) is the online portal for external users (clients, ARs, and agencies). This portal includes the:

* Online application for Health Coverage, SNAP, and TANF
* Screening Tool
* Access to case status
* Print Proof of Eligibility
* Print Paper Application
* Credentials for clients, ARs, and agencies to securely access Benefits Portal
* DFR Helpdesk access to Administrative Portal component for supporting clients, ARs, and agencies with credential issues (e.g., password reset, lost user ID)
* Health Coverage Online Application for E&E Workers to enter Health Coverage Telephone Applications on behalf of clients, ARs, and agencies (secure access for E&E Workers using their State-issued IDs via State LDAP)
* Important E&E program and/or access information

|  |  |
| --- | --- |
| **Interfaces** | Document Center, I3/IVR, IMPACT, Worker Portal, IEDSS, Data Warehouse, Managed Care Entities (MCEs) to support Fast Track Eligibility Credit Card Payments |
| **Users** | Clients, ARs, agencies for Online Application, Screening Tool, Access to case status, Print Proof of Eligibility, Print Paper Application.  E&E Workers for Health Coverage Online Application supporting Health Coverage Telephone Applications on behalf of clients, ARs, and agencies.  DFR Helpdesk users supporting clients, ARs, and agencies with credential issues. |
| **Technology** | * Java frameworks * Docker / containers * MongoDB |
| **Notes** | * Support E&E Workers in providing role-based access to the Health Coverage Online Application supporting Health Coverage Telephone Applications on behalf of clients, ARs, and agencies * Support DFR Helpdesk in facilitating their role based access to the Administrative Portal component for supporting clients, ARs, and agencies who encounter credential issues (e.g., password reset, lost user ID) * Fast Track Eligibility Credit Card Payments are supported via interfaces to MCEs in Indiana. When applicants apply for Health Coverage, in the event that they are eligible for HIP 2.0 and Fast Track Eligible, their credit card payment can be collected for immediate Power Account (PAC) payment in support of HIP 2.0 coverage * See Attachment J for Benefits Portal Architecture |

* 1. **Workstream 2 - Agency Portal M&O**

The Agency Portal is the online portal for agencies to monitor important eligibility determination status information about clients that they serve. See <https://www.in.gov/fssa/dfr/4323.htm> for details.

|  |  |
| --- | --- |
| **Interfaces** | Worker Portal, IEDSS, Data Warehouse |
| **Users** | Agencies, Contractor |
| **Technology** | * Java frameworks * Oracle 12c on Exadata |
| **Notes** | * The Contractor is responsible for supporting the processes for agencies to be registered as an Agency Portal user * See Attachment J for FACTS System Component and Internal Channel Diagram |

* 1. **Workstream 3 - CDMS M&O**

The CDMS components are the mechanisms for integrating and interfacing AS solution components to work with IEDSS and legacy systems.

|  |  |
| --- | --- |
| **Interfaces** | Worker Portal, Benefits Portal, Document Center, IEDSS |
| **Users** | Contractor, Systems (interfaces), administrative users for document access |
| **Technology** | * Java frameworks * Oracle 12c on Exadata |
| **Notes** | * See Attachment J for the CDMS Environment Architecture, the CDMS Network Diagram, and the DPS architecture Diagram * Includes linkage to IEDSS Worker Portal and Benefits Portal |

* 1. **Workstream 4 - Document Center M&O**

This functionality is necessary for supporting E&E and E&T documentation issued to or returned by clients, ARs, and agencies. The Document Center has functionality for intelligent barcoding for routing documents by type and to particular cases. Additionally, some forms have OCR functionality configured.

|  |  |
| --- | --- |
| **Interfaces** | Worker Portal, Benefits Portal, Document Center, ICES, CDMS, IEDSS |
| **Users** | Staff with the document center services vendor, which currently is Phoenix Data Corporation |
| **Technology** | * Captiva (refer to the DDI description Section 7.10 for Captiva upgrade/replacement) * IBM Content Manager (refer to the DDI description Section 7.10 for IBM Content Manager replacement) * Oracle 12c |
| **Notes** | * Maintain Captiva templates, including OCR configuration, and linkage to Cúram worker portal with indexing via Oracle. The format of documents must be managed with the BA team and support State forms formatting requirements as dictated by FSSA, DFR, and IARA (<https://www.in.gov/iara/2362.htm>). Support the document center services vendor directly for support their users require with document processing |

* 1. **Workstream 5 - IMPACT M&O**

This functionality is necessary for supporting the DFR E&T program, IMPACT. IMPACT casework, including scheduling, work activity tracking, and compliance with E&E requirements are all included within this solution.

|  |  |
| --- | --- |
| **Interfaces** | Worker Portal, Document Center, ICES, CDMS, IEDSS, Data Warehouse |
| **Users** | IMPACT workers, E&E workers |
| **Technology** | * Java frameworks * Oracle 12c |
| **Notes** | * See Attachment J for the IMPACT Architecture Diagram * Maintain SNAP and TANF E&T outcome reports as well as the data feed to Data Warehouse for all applicable IMPACT reporting that they conduct * Support IMPACT workers in providing role based access to the system |

* 1. **Workstream 6 - I3/IVR M&O**

This functionality is necessary for supporting the call center functionality for E&E and E&T workers and clients/ARs/agencies to interact. The IVR functionality drives self-help and automated functionality, while also providing routing for clients/ARs/agencies to interact directly with workers via queue-driven call routing (by region, by worker type, by availability). The Contractor will make reporting available to the State via this platform for call center-oriented metrics.

See Attachment J’s “Att J-5I3-IVR Genesys PureConnect System Overview.pdf” for high level system diagram information. Page 1 of this pdf includes the entire high level system diagram view for production, non-production, and disaster recovery elements. Page 2 of this pdf clarifies the details of the production environment, including information on each major component, their interfaces, as well as who is responsible for supporting (i.e., Contractor versus IOT). Note: FACTS and ICES on top right of PDF are replaced by IEDSS.

|  |  |
| --- | --- |
| **Interfaces** | Worker Portal, ICES, CDMS, IEDSS, Data Warehouse |
| **Users** | E&E and E&T staff |
| **Technology** | * Genesys PureConnect I3 on premise solution * Java frameworks / .NET * DB2 |
| **Notes** | * The Contractor must maintain handlers and the IVR database. They must support these solution components in conjunction with IOT who maintains the platform itself. * The Contractor must provide an experienced and certified Genesys PureConnect configuration and development specialist for the support and maintenance of the DFR phone system solution. This resource must be capable of supporting standard and custom handlers, with specific concentration in IVR, Automatic Call Distribution (ACD), and Auto Dialer. This resource shall be responsible for participation in scoping and requirements sessions, design, development, defect resolution, and production deployment and support per State security guidelines. Areas of focus include the optimization of the DFR IVR and phone system solution; the support of efforts to decrease custom handler usage, streamline IVR prompts and messaging, and maintain self-service functionality and integration with source solutions; and the requirement to work closely with IOT Contact Center Support and IOT Server Support for all production changes and new development efforts. |

# **DDI, Enhancements, and Change Management**

* 1. **Overview**

The Contractor shall provide enhancement services throughout the Contract term. Enhancements may be required for any of the components under M&O or a new AS solution component. Enhancements will be managed via the Change Management Process (See Section 7.2). All SDLC activities will be considered enhancements. The number of Contractor enhancement staff and type of enhancement services the Contractor provides at any given time will depend on the State’s enhancement needs and rollout schedule. The Contractor shall proactively work with the State in status meetings and through other notification opportunities to identify upcoming enhancement needs so that the Contractor shall be prepared to take on the additional work. Any staffing constraints should be discussed with the State as soon as the Contractor is notified about the enhancement need.

During the IEDSS rollout, the Contractor may be called upon to support ongoing testing and other related activities to support IEDSS testing or issue resolution upon request from the IEDSS vendor or the State (e.g., UAT). The support for this type of activity falls under this section. Following IEDSS rollout, these activities would fall under M&O workstreams as noted in the previous section.

* 1. **Change Management**

Integrated Change Management is the process of reviewing all change requests and approving and managing changes to evaluate the impact to time, cost, and quality. Having a well-defined and robust Change Management Process is crucial to the AS solution because of the multiple end user organizations involved. For all SDLC activities within the Contract scope, the following change management activities are required:

* The Contractor shall analyze, size, and provide proposal / cost estimates.
* The State will review estimates and either approve or disapprove changes based on estimates, priority, and other factors.
* The State will clarify priority and impact on existing enhancements and other change requests.
* The Contractor shall work with the State to update project documents.
* The Contractor shall work with the State to communicate status to stakeholders.
* Both the State and the Contractor shall monitor outcomes.

Any Contractor requests for changes to approved deliverables, hardware, software, processing, procedures, manuals, forms, reports, and other artifacts will follow the same Change Management process.

AS solution components are expected to respond efficiently and effectively to the need for changes stemming from the ever-increasing complexity of the health care and social services environment brought about by policy changes at the local, State, and Federal level. To stimulate and support innovative responses to the demand for change, the Contractor is required to actively participate in the change evaluation process and ensure that they analyze and understand the impact of all changes regardless of the originating party.

Example CRs have been included in Attachment K for an understanding of the level of information typically necessary for CR documentation.

* + 1. **Change Management Process**

**Overview**: The Change Management process for AS is mature and already supported with a process, electronic forms (Atlassian Jira portal) with required fields, and a Steering Committee with regular meetings and Communication Plan. The Contractor will be provided access to all of these processes and the State’s Jira portal to support their role in Change Management.

The State shall issue a Change Request (CR) within this Contract’s scope that the Contractor shall perform. The Contractor shall respond to the CR with a Change Impact Analysis, triggered by request from the Steering Committee. Once the Change Impact Analysis has been approved for implementation (including any modifications made during the review process), the Change Impact Analysis shall be deemed an approved CR. The Contractor shall not begin work on any CR prior to receiving this State approval.

**CR Contents:** The CR will include:

* Description of proposed Change, including requirements
* Justification of Change
* CR implementation date
* The State’s decision as to whether the CR will utilize a fixed fee or time and materials-based pricing Anticipated work location(s) and non-standard work hours, if applicable
* Deadline for Contractor to provide a Change Impact Analysis
* Applicable program/funding source for the Change

**Change Impact Analysis:** Within fifteen (15) days (or such longer period as the Contractor and the State may mutually agree) following receipt of a CR, the Contractor shall prepare and deliver to the State and the Steering Committee a written Change Impact Analysis, in form and substance acceptable to the State. At a minimum, a Change Impact Analysis will be a written assessment and evaluation of the impact of the proposed Change on the then current scope, price, and performance of the services in accordance with the time schedule agreed between the Contractor and the State. It must include the following, at a minimum:

* Description of the proposed Change
* Justification of the proposed Change
* Whether the Change is part of a Maintenance Release (MR), not part of a Maintenance Release (Non-MR), or an enhancement
* Staffing plan (organization chart, staff names and titles) and cost breakdown (hours by individual multiplied by contractual rates)
* Staffing projection analysis, with supporting documentation, of the reasons the Contractor believes the fees will be materially impacted by the proposed Change
* An analysis of the impact of the proposed Change on the following (as appropriate given the nature of the proposed Change):
  + Scope of the Contract
  + Projected or anticipated savings, if any
  + Performance standards
  + Delivery dates
  + Security impacts and how they will be addressed
  + Any other matter reasonably requested by the State or reasonably considered by the Contractor to be relevant
* A list of work products or deliverables that the Contractor will submit to implement the proposed Change
* A timetable for implementation of the proposed Change
* An assessment of the added value of a proposed Change to the State and to meeting the policy objectives
* Anticipated work location(s) and non-standard work hours, if applicable
* SLAs and any performance withholds or incentives in addition to those in the Contract.

**CR Approval:** The Contractor and the State will cooperate with each other in good faith in discussing the scope and nature of each CR and related Change Impact Analysis. The Steering Committee will meet to discuss the CR, Change Impact Analysis, and any other matters concerning the Change to determine to approve, defer, or cancel the pending CR. In the event that more than one CR is pending concurrently, the Steering Committee shall establish the priority and sequence for addressing such changes. The State will approve and execute a written CR containing a description of the change, the pricing, any anticipated increase or decrease in workload which may be caused to comply with such change once implemented, a timeframe for implementing the change, and any modification to any of the contract documents to reflect such change as the Contractor and the State shall mutually agree.

The State reserves the right to condition the approval of any CR on the review, input, and approval of any governmental body that the State deems appropriate with respect to the CR.

Please see Attachment K, “Att K-5 Sample CR 1.pdf” and “Att K-6 Sample CR 2.pdf” for a sample Change Request document. This document illustrates the level of information required in Change Request documents.

* 1. **Enhancements Pool**

The Contractor shall provide a capped Enhancements Pool of 132,000 hours a year (estimated 11,000 hours per month). The State is not required to use up the hours and dollars allocated for the Enhancements Pool for each State Fiscal Year. Please see Section 7.8 for more information on Minor Changes that do not draw from the Enhancements Pool.

Changes that are needed to fix an enhancement after it is implemented and that are brought to the Contractor during the Software Warranty period will not count towards the Enhancements Pool. Please see Section 7.5 for information about the Software Warranty.

* 1. **Enhancement Pricing**

Enhancement pricing will either follow the fixed fee deliverables-based approach or the time and materials-based approach based on Contractual hourly rates. The State will determine the method to use for each enhancement through the Change Management Process. If services are provided in exchange for fixed or not-to-exceed compensation, the Contractor is solely responsible for any costs in excess of the specified compensation.

The maximum hours invoiced for an individual shall not exceed 45 hours a week, regardless of the number of hours worked by the individual to meet service levels and complete deliverables on time.

* 1. **Software Warranty**

The State requires a 90-day warranty for all modifications and enhancements made to AS solution components. The Contractor shall fix no additional cost to the State (1) any post-production defects discovered during the 90-day warranty period and (2) any defects discovered during the 90-day warranty period that arise in a previously working component due to the rollout of a new change or enhancement. The hours required for the fixes will not count against the Enhancements Pool hours. Fit functionality in relation to user requests and agreed to specifications will be tracked by the State. Action may be taken to address consistently poor performance.

* 1. **Right to Contract with Other Service Providers**

Notwithstanding any other provision of this Agreement, the State retains the right to contract with one or more service providers for any matters that would be the subject of a CR.

* 1. **Priority of Change Requests**

In the event the State or the Contractor reasonably determines that all CRs that are in the process of implementation and which require actions to be taken by such party cannot be accomplished within the timeframes for such CRs, or which would be impractical to implement at the same time due to workload constraints and other relevant factors, the priority in which the CRs shall be worked shall be determined by the State.

* 1. **No Cost Impact: Routine Changes and Software Warranty**

Routine changes made in the ordinary course of the Contractor’s provision of M&O services defined within the scopes of the Contract shall be made at no additional cost to the State. Examples of routine changes that are included in the routine M&O of the AS solutions and be performed at no additional cost to the State are:

* Activities necessary for AS solution components to (a) function in compliance with Federal and State laws and administrative rules, the State Plan, State waivers, State policies, and the operating manuals in effect at the time of proposal submission and (b) to correct deficiencies found after implementation of modifications. The State expects AS to maintain continual Federal and State regulation compliance
* Activities necessary to comply with new industry standards and operating rules associated with those standards
* Changes to operating procedures, schedules, and equipment configurations.
* Activities necessary for the solution to meet the contractual performance requirements
* Activities necessary to ensure that data, tables, programs, and documentation are current and that errors are found and corrected
* Data maintenance activities for updates to tables, including database support activities
* Changes to scripts or solution parameters concerning the frequency, number, sorting, and media of reports

All CRs are considered either covered under the Software Warranty (See Section 7.5) or are no-cost maintenance CRs unless the State approves additional compensation through the Change Management process. Determination of such status including Contractor dispute of status shall not delay the implementation of the CR.

* 1. **Time Tracking**

By the tenth day of each month, the Contractor shall provide an electronic report of actual hours worked by position and activity by approved enhancement. After the completion of an enhancement, the Provider will provide an enhancement-specific report of actual hours worked by position and activity within fifteen (15) days of the completion of the enhancement. The State will check invoice details before the invoice is processed. See Section 4.5.2 for details on time reporting.

* 1. **Anticipated Enhancements**

The State anticipates that the Contractor will be asked to execute several enhancements to the AS solution. The following are the currently anticipated enhancements. The Contractor must not begin any work on an enhancement until the related CR is approved by the State.

* **Benefits Portal functionality deferrals.** CRs will be made available to the Contractor regarding these pending items.It is anticipated that design documentation and SDLC artifacts may be in progress that can be prioritized for finalization upon Contractor engagement
* **Hoosier Digital Link LDAP.** Implement Hoosier Digital Link LDAP for external user credentials (clients, ARs, agencies)
* **IBM Content Manager replacement for Document Center DDI.** Leverage solution components and SDLC artifacts that have been created to date for this effort by the current vendor, and complete implementation. Recommend a cost-effective method to meet Document Center requirements that have been realized with IBM Content Manager. The full functionality of IBM Content Manager has not been necessary, so simpler tools and architecture will be considered
* **Captiva upgrade/replacement.** The State’s version of Captiva is anticipated to be at end of life within the term of this agreement. Consequently, the State expects the Contractor to work with the State on an alternatives analysis to determine the optimal upgrade and/or replacement path. The Contractor will support implementation of the State’s chosen path

# **Training**

As a part of the training responsibilities of this contract for all scope, the Contractor shall provide:

* **Solution Usage Training:** While the Contractor is not responsible for creating training artifacts or delivering training content of this type, they will be expected to answer or clarify design or system questions that may arise as the State conducts training activities.
* **SDLC and PM Processes Training:** Provide training on the SDLC methodologies for State and partner staff who become involved in the SDLC process facilitated by the Contractor. A significant focus of this training would be how State leadership and State subject matter experts (SMEs) are involved throughout each phase of SDLC efforts.
  + At no cost to the State, the Contractor is expected to facilitate and support training of their own staff to ensure that they are up-to-date on SDLC best practices, technology best practices, and other related training available for current or proposed technologies and processes under AS solution components.
* **Security Training:** Provide required security training for the Contractor’s staff (see Section 5.8, Section 10.1, and Attachment B, Section 12).

# **Transition and Turnover**

**Initial Transition**

Prior to taking over the scope noted in this RFP, the Contractor shall work with the State to develop and manage plans for transferring services from the incumbent vendor over a 60-calendar day period. As a part of the Initial Transition Period, the incumbent vendor will leave behind all solution documentation (requirements, design, BPMs, UI specs, form specs, architecture documents, and MR/non-MR/security reporting) for the AS solution on the State’s instance of SharePoint as well as requirements, configuration, build configuration, and other related information within the State’s maintained ALM. This strategy is true for both the items within the scope of M&O as well as any in-progress DDI artifacts and solution components.

**End of Contract Turnover**

The State seeks to ensure that program stakeholders experience no adverse impact from the transfer of scope to either the State or to a successor contractor when the Contract is complete or terminated early. In addition to the requirements in Attachment B Contract clause 13 (Continuity of Services), the following end of Contract turnover requirements apply:

* Six (6) months prior to the end of the base Contract period, the Contractor must develop and implement a State-approved Turnover Plan covering the possible turnover of the AS solution or operational activities to either the State or a successor contractor. The Turnover Plan must be a comprehensive document detailing the proposed schedule and activities associated with the turnover tasks. The plan shall describe the Contractor's approach and schedule for transfer of all SDLC artifacts and documentation created, maintained, and updated throughout the Contract term on the State SharePoint site and/or ALM. The information must be supplied on media specified by the State and according to the schedule approved by the State. Turnover task requirements and approximate timeframes are provided in the sections below. The dates and data requirements in the following sections are illustrative only and do not limit or restrict the State's ability to require additional information from the Contractor or modify the turnover schedule as necessary.
* Four (4) months prior to the end of the base Contract period, or any extension thereof, the Contractor must transfer the following information to the State or its agent on a medium acceptable to the State:
* A copy of non-proprietary solution components or database(s) used. Please see the Section 26 (Ownership of Documents and Materials) in RFP Attachment B (Sample Contract) for requirements regarding ownership of work products;
* Internal logs and balancing procedures used during the contract to ensure compliance with operational requirements; and
* Other documentation including, but not limited to, user, provider, and operations manuals, and documentation of any interfaces developed to support business activities between contractors.
* Four (4) months prior to the end of their contract or any extension thereof, the Contractor must begin training State staff or its designated agent's staff, in the operations and procedures performed by Contractor staff. Such training must be completed at least two (2) months prior to the end of the Contract. The State’s turnover of services to the new contractor will take place two (2) months prior to the end of the contract. The Contractor shall be available for the last two (2) months of the contract to provide support as requested by the State. This support will be invoiced according to the contractual hourly rates.
* The Contractor shall appoint, with State approval, a Turnover Manager who will manage and coordinate all Turnover activities (see Attachment I for Program Manager 1 who can do this work). The Contractor shall submit their manager's qualifications as part of their Turnover Plan. The Contractor shall not reduce operational staffing levels during the turnover period without prior approval by the State. The Contractor shall not in any way restrict or prevent Contractor staff from accepting employment with any successor contractor. The State will work with the Contractor and successor contractor on the timing of any transition of Contractor staff. The Contractor shall provide to the State, or its agent, within fifteen (15) business days of request all updated data and reference files, scripts, and all other documentation and records as required by the State or its agent.
* If the optional Contract terms are exercised during turnover activities, these turnover activities shall shift to the next year. If the turnover is halted due to the State exercising an optional term extension, invoices will not include Turnover Manager costs after the State's date to halt turnover activities until those activities resume (with the State's approval) in the following year.

Turnover costs will only include the Turnover Manager’s costs. Any additional staff costs shall be covered by the M&O fees unless otherwise approved by the State.

# **Compliance with Standards & Regulatory Requirements**

For a complete list of contractual expectations, see Attachment B.

The Contractor must ensure their systems comply with all State and Federal laws and regulations, including but not limited to the Americans with Disabilities Act (ADA), the Balanced Budget Act (BBA) of 1997 Subtitle H, and the Medicaid Managed Care rules, 42 CFR 438. The Contractor must also comply with FSSA Security Policies (<http://www.in.gov/fssa/4979.htm>).

* 1. **Privacy and Security Standards**

The State of Indiana requires that all vendors comply with all current and future HIPAA privacy rules and the applicable privacy controls under Minimum Acceptable Risk Standards for Exchanges MARS-E Version 2.0 (and all subsequent versions), as well as other State and Federal laws and regulations as they relate to protecting the privacy of and security over citizen information in the Contractor’s safekeeping.

Additionally, the Contractor shall comply with relevant security and privacy policies and requirements, including but not limited to the following:

1. Policies and requirements in Attachment B, Section 12
2. FSSA Application Security Policies and Standards (<http://www.in.gov/fssa/4979.htm>)
3. State of Indiana Code (IC) Title 4
4. OWASP Application Security Verification Standard 3.0 (<https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf>)
5. FSSA Security Assessment Policy (<http://www.in.gov/fssa/files/FSSA_Security_Assessment_Policy.pdf>)
6. IOT Policies, Procedures, and Standards (<http://www.in.gov/iot/2394.htm>) including the IOT Information Security Framework (<http://www.in.gov/iot/files/Information_Security_Framework.pdf>)
7. State of Indiana security requirements found in IC 4-1-6,
8. Applicable safeguard requirements for:
   * SNAP information under 7 CFR §272.1(c) and within the [Food and Nutrition Service (FNS) handbook 901](https://fns-prod.azureedge.net/sites/default/files/apd/FNS_HB901_v2_Internet_Ready_%20Format.pdf) (including Chapter 9, Systems Security)
   * TANF information under 45 CFR §205.50 and IC 12-14-1.
   * Medicaid information under 42 CFR Subpart F and IC 12-15-27
   * Vocational rehabilitation information under 34 CFR §361.38.
9. FSSA’s security standards found at: <http://www.in.gov/fssa/4979.htm>
10. HHSS IT Access Control Standard and MARS-E 2.0 (and subsequent versions) requirements for unique user identification (UUI). UUI access and security roles are assigned by FSSA Account Control in conjunction with IOT security administrators.
11. IOT’s Information Resources Use Agreement (IRUA) found at: <https://www.in.gov/iot/IRUA.htm>
12. IOT standards regarding encryption of all communications (FIPS 140-2). Encrypt all data stores to the FIPS 140-2 standard.

For a complete list of contractual expectations, see Attachment B, Section 12.

With regards to privacy and security standards, in addition to compliance with the above policies and requirements, the Contractor shall:

1. Uphold the State’s privacy guarantees as documented in Indiana Code 5-14-3: <http://www.in.gov/legislative/ic/code/title5/ar14/ch3.html>.
2. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI and PII that the Contractor creates, receives, maintains, or transmits on behalf of the State of Indiana.
3. Mitigate, to the extent practicable, any harmful effect that is known to the Contractor of PHI and PII obtained under this contract in a manner not provided for by this Contract or by applicable law of which the Contractor becomes aware,
4. Ensure that any subcontractors or agents to whom the Contractor provides PHI or PII received from, or created or received by the Contractor, and subcontractors or agents on behalf of the State, agree to the same restrictions, conditions, and obligations applicable to such parties regarding PHI and PII.
5. Report to the State any security and/or privacy incident of which the Contractor becomes aware. Please see Section 5.8 for additional details.
6. Train all staff on the privacy rules and requirements (The Contractor shall develop and provide to its staff applicable training with the successful completion of such training on no less than an annual basis; in addition, Contractor staff will need to undergo specific State-provided privacy and security training upon first hire and then on no less than an annual basis.)
7. Use available Security Architecture assets in constructing AS solutions.
8. Perform access authentication against the IOT-managed Active Directory (LDAP) service for all access (user and service accounts).
9. Establish the AS solution components’ access control (authorization) in compliance with MARS-E 2.0 (and subsequent versions). The AS solution components’ access control must be based on unique roles (role-based security) defined for that user.
10. Apply all security patches to the software and hardware it controls on a timely basis. Ensure that all hardware have relevant anti-virus and anti-spyware software to ensure a safe operating environment.
11. Ensure operating system and AS solution component audit logs are generated in accordance with MARS-E 2.0 (and subsequent versions) (reference AU controls); audit logs must be retained online for no less than 90 days and retained in accessible archive storage for no less than 10 years. In addition, Contractor will facilitate audit log integration with the State’s SIEM solution for event correlation, analysis, and alert functions.
12. Support the Federal automated data processing requirements, such as 42 U.S. Code § 654a - automated data processing​. The Contractor will also support and comply with new FSSA and IOT initiatives and directives regarding new or enhanced security measures. IOT has instituted the concept of three-tier Protected Zones, to isolate applications, data, and presentation services within the State network, including AS solution components. These security measures necessitate enhanced access controls requiring two-factor authentication, the employment of VPNs, and stringent firewall protections with “default deny” configurations, which may have an impact on system administration and operational use procedures.
13. Work with IOT, DFR, and FSSA Privacy & Security to secure all non-production and production environments (e.g., development, integration testing, performance testing, user acceptance testing, production staging, and production) according to all required security standards. As a matter of policy, production data cannot be used for testing unless such data is masked to the extent that any improper use or disclosure of such data would not constitute a breach under Federal and State laws and regulations. Further, the Contractor’s design of the AS solution must address the MARS-E 2.0 (and subsequent versions) and FSSA policy requirements for data minimization.

Also see Section 5.8 for additional Security support requirements.

* 1. **Business Continuity and Disaster Recovery**

The Contractor is required to comply with and maintain the existing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) and support DFR and IOT in updating these plans, as applicable, based on evolution of data, infrastructure/architecture, and tools.

* + 1. **Business Continuity**

The BCP must provide adequate backup and recovery for all operations, both manual and automated, including all functions required to meet the backup and recovery standards: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). At a minimum, the BCP shall document the following:

|  |  |
| --- | --- |
| **Overview** | * Identify all critical information areas * LAN/WAN * Telecommunication * Applications and data * Identify potential disruptive events * Staff duties * Manmade events |
| **Scope and Plan Initiation** | * Describe operations (Contractor, State) * Create detailed account of work * List resources * Define management practices * Define roles and responsibilities * BCP Committee * Senior Management |
| **Business Impact Analysis (BIA)** | * Address three primary goals:   1. Criticality prioritization   2. Downtime estimation (maximum tolerable downtime) not to exceed thirty (30) calendar days in the event of a catastrophic or natural disaster; not to exceed ten (10) calendar days in the event of other disasters caused by such things including but not limited to criminal acts, human error, malfunctioning equipment or electrical supply   3. Resource requirements * BIA Results * Assessment materials gathering * Vulnerability assessment * Quantitative loss criteria * Qualitative loss criteria * Information Analysis * Results and recommendation |
| **BCP Development** | * Recovery Plan * Continuity Strategy |

The Contractor shall support ongoing testing and validation of the BCP at a minimum, annually.

Current State BCP artifacts will be presented to the Contractor at the beginning of the Contract term.

* + 1. **Disaster Recovery**

The Contractor shall support ongoing testing and validation of the DRP. The State will not acknowledge that recoverability exists until the plan is tested and it is able to verify the accuracy of the plan. The DRP must present:

1. Statement of actions taken before, during, and after a disruptive event
2. Procedures required to respond to an emergency, providing back-up operations during a disaster

At a minimum, the DRP must include the following:

|  |  |
| --- | --- |
| **Overview** | Goals and Objectives |
| **Data Processing Continuity** | Describe the consideration and ultimate selection of the following backup systems and facilities:   * Reciprocal (mutual aid agreements) * Subscription services * Hot site * Warm site * Cold site * Mobile site * Multiple centers * Transaction redundancy * Electronic vaulting * Remote journaling * Database shadowing * Backup and maintenance schedule |
| **Testing** | Describe the consideration and ultimate selection of the following:   * Testing checklist: how you will distribute the DRP for review * Structured walkthrough: how you will walk all business managers through the test plan review * Simulation: all involved people conduct practice sessions * Parallel: primary processing does not stop * Full interruption: cease normal operations |
| **Recovery Procedures** | * Describe Recovery Team duties * Implement the recovery procedures in a disaster * Assure critical functions operating at backup site * Retrieve materials from offsite storage * Install critical systems and applications * Describe Salvage Team duties separate from recovery team * Return primary site to normal operating conditions * Clear and repair primary processing facility * Describe Normal Operations Team, returning production from disaster recovery to primary * Address other recovery issues * External groups * Employee relations * Fraud and crime * Financial disbursement |

The Contractor must conduct a disaster recovery exercise once a year to confirm disaster recovery functionality and document the results with an action plan for correcting issues found during the disaster recovery exercise.

Current State DR artifacts will be presented to the Contractor at the beginning of the Contract term.

# **Staffing**

* 1. **General Staffing Requirements**

The Contractor shall develop and adhere to an approved Staffing Plan that addresses their resource plans during the entire Contract term. Specifically, the Staffing Plan shall include the following:

* 1. Number, type, and categories or staff proposed
  2. Staff qualifications
  3. Staff work location
  4. Plan for new or reassigned staff that includes:
* Recruitment of new staff
* Staff transition

The Contractor is expected to use individual staff to cover multiple M&O Services and enhancement efforts to the greatest extent possible, while not sacrificing quality of service, including SLAs. These services are not anticipated to be provided in “silos”, and efficiencies in staffing are expected.

During the Contract term, the State reserves the right to require replacement of any Contractor or subcontractor employee found unacceptable to the State. Reasons for unacceptability include, but are not limited to, the inability of the individual to carry out work assignments or unsatisfactory job performance as determined by the State. The individual must be removed within two (2) weeks of the request for removal, or sooner if requested by the State, and be replaced within thirty (30) calendar days after the position is vacant, unless a longer period is approved by the State.

As a part of the staffing responsibilities, the Contractor shall:

* 1. Update the Staffing Plan annually for approval by the State.
  2. Perform criminal background checks for Contractor staff at no additional cost to the State. Submit for review results of criminal background checks for Contractor staff to the State.
  3. Identify and immediately dismiss any employee with a background unacceptable to the State.
  4. Identify, report, and resolve performance issues for its entire project staff including but not limited to employees and subcontractors.
  5. **Key Personnel**

Key Personnel are Contractor staff members deemed by the State as being both instrumental and essential to the Contractor’s satisfactory performance of all contract requirements. The following general provisions apply to Key Personnel:

1. Employed full-time and have their primary workplace location within the greater Indianapolis area (see Section 11.4.5)
2. Staffed by one and only one specific individual at any given point in time. That is, it is not permissible to have multiple Contractor staff perform one Key Personnel position’s responsibilities unless approved by the State
3. Key Personnel are subject to approval by the State. As part of their Staffing Plan, the Contractor shall have named backup Key Personnel in the event of a prolonged illness or unexpected absence/departure who can be take over the vacated role within two (2) weeks of the Key Personnel’s absence or departure. The Contractor shall receive State approval before replacing any Key Personnel or backup Key Personnel. The Contractor may not make any temporary or permanent changes to Key Personnel or backup Key Personnel without at least four (4) weeks prior notice to the State and the State's prior written approval unless the replacement is due to termination, death, or resignation. The Contractor shall replace Key Personnel with personnel of equal or greater ability and qualifications, subject to approval by the State, regardless of the reason for replacement

The Key Personnel positions and responsibilities listed in Attachment I are considered essential. The general responsibilities and minimum qualifications cover the State’s minimum expectations. To accommodate differences in organizational structures or if a Respondent believes that an alternative organizational design could improve service levels or decrease costs, the State will consider suggestions for alternative alignment of duties. Changes to the positions and responsibilities will only be allowed with written permission from the State.

For the contract, Key Personnel are indicated on Attachment I.

* 1. **Other Essential Personnel Requirements**

The State requires that the Contractor maintain other essential personnel who assist and support the Key Personnel. Duties of other essential personnel will largely be left to the determination of the Contractor, as the Contractor is best situated to make this determination.

* 1. **Facilities and Equipment**
     1. **Facilities and Parking**

The Contractor’s facilities shall be located in the Greater Indianapolis area for the duration of the Contract. The Contractor shall be fully responsible for the costs of their facilities (including but not limited to leasing costs, parking fees, and utilities) and these costs will not be reimbursed by the State.

* + 1. **Hardware, Software, Accessories, and Peripherals**

With the two exceptions listed in the next paragraph, the Contractor shall supply all hardware, software, accessories, and peripherals for their staff (including any subcontractor staff) that will be necessary to complete the requirements of the Contract.  The Contractor shall not invoice the State for these costs. The Contractor is responsible for ensuring use and management of all hardware, software, accessories, and peripherals are compliant with IOT policies, FSSA policies, applicable Indiana policies, and MARS-E 2.0 (and subsequent versions) /HIPAA requirements (for example, in terms of encryption, audit logging, audit processes, and antivirus protection). See Attachment B, Section 12 for all confidentiality, security, and privacy of personal information requirements to which the Contractor must adhere.

The only exceptions will be:

* Adobe Lifecycle, Captiva, and Cúram workstation licensure necessary for staff to execute the scope of the Contract. This licensure will be provided by the State. Additionally, as noted in Section 2.6, the State is maintaining all required server software and hardware
* Virtual Private Network (VPN) access to the State network. This expense will be covered by the State
  + The Contractor shall connect to the State over the Internet via a site-to-site VPN connection, which will be provided and managed by the State.
  + The Contractor shall manage network infrastructure at the site and support the site’s network connecting to the State’s VPN.
  + Host access will be based upon access-lists in the VPN appliance maintained by the State.
* The Contractor is free to provision, manage, and control any device at the site, but within IOT and FSSA policies. See Attachment B, Section 12 for all the confidentiality, security, and privacy of personal information requirements to which the Contractor must adhere.
  + 1. **Office Supplies**

The Contractor shall be fully responsible for providing all office supplies to their employees (and subcontractor employees) for the necessary completion of the requirements of this RFP.  This includes but is not limited to office furniture, paper, and envelopes. The Contractor shall not invoice the State for these costs.

* + 1. **Multifunctional Printers**

**Multifunctional Printer Configured for Document Center SDLC:** The State shall provide the Contractor with a multifunctional printer (MFP) device that is customized in alignment with the MFPs in use in the field (i.e., DFR operations offices, such as Local Offices and Regional Change Centers) and in Document Center operations. This MFP is customized further for SDLC purposes by allowing documents to be directed to any non-production environment. In other words, developers and/or testers can scan documents and then direct them to the desired environment.

The State shall only provide one device for such purposes. If the Contractor requires more, each additional device must be justified and will require written State approval.

**General Use MFPs:** Any other MFPs, regular printers, scanners, and similar devices required by the Contractor for general purposes shall be the full responsibility of the Contractor. The State will not reimburse the Contractor for any of these devices.

* + 1. **Personnel - Geographic Requirements**

Worksheet 1, Attachment I of this RFP include designations of which Contractor staff positions shall be required to be full-time at the Contractor’s Greater Indianapolis facility. These personnel will be required to attend any meetings Monday through Friday, 8:00AM to 5:00PM (with the exception of official State holidays) when requested by the State. Positions that are not designated specifically as within the Contractor’s greater Indianapolis facility must be located in the United States. Temporary exceptions to these requirements will require prior approval from the State.

* 1. **Subcontractors**

The Contractor shall be fully responsible for managing all subcontractors used to execute the services of the Contract. The subcontractor(s)’s compliance with all requirements, terms, and conditions shall be the responsibility of the Contractor.

# **Service Level Agreements**

* 1. **Service Levels Overview**

Failure by the Contractor to meet Service Level Agreements (SLAs) may cause the State to incur economic damages and losses, including but not limited to:

* Federal penalties
* Lost Federal match funding if certain implementation deadlines are missed
* Staff productivity losses due to downtime/poor response times
* Costs incurred due to any overtime necessitated
* Applicant time lost if interface is partially or completely down
* Impact on other State systems due to downtime or other processing issues
* Negative project impact and/or risk of negative audit findings due to lack of proper documentation or improper procedures
* Impact to timeline/budget due to unavailability of key staff resources and/or adequate resources on site

As such, compensation to the Contractor will be tied to the SLAs below. The Contractor will provide periodic (monthly and quarterly) updates on their performance in relation to the SLAs. FSSA will hold the Contractor accountable to these SLAs and failure to meet SLAs on a consistent basis could have a significant impact on compensation levels to the Contractor (please see Performance-Based Withholds in Section 12.2.1 and Section 12.3.2).

* 1. **Maintenance and Operations Service Levels**

The following are service levels for M&O services. All service levels will be reported monthly to the State in a written report, per Section 4.5.1 and in claims submitted. Validation of the SLAs will be conducted by the State and/or the OV&V Contractor, and the Contractor must provide any supporting documentation requested as part of validation activities. The Contractor shall provide full transparency via the State SharePoint site and/or ALM to access all materials and associated work products, including but not limited to staff time reports, staff status reports, staff calendars, agendas, meeting notes, charters, and request trackers.

* + 1. **M&O Performance-Based Withhold**

1. **M&O Thresholds for Compliance**

The table below provides the SLA thresholds that define compliance and are the basis for determination of loss of the performance-based withhold of the monthly M&O fee.

| **SLA#** | **Key Service Level Agreement** | **Threshold for Compliance (Reported Monthly)** |
| --- | --- | --- |
| 1 | **System Uptime.** Maintain AS solution components’ system uptime against a 24-hours per day, 7 days per week operating schedule, excluding scheduled maintenance time.  Note: Any maintenance exceptions should be either for a standing window (such as 2:00 A.M. to 4 A.M. on Sundays) or have written pre-approval from the State. | 99.99% uptime other than scheduled maintenance time. |
| 2 | **Helpdesk Resolution Timeliness.** Resolve opened helpdesk tickets in the required timeframes outlined in Section 5.6.6.2 to the satisfaction of the State | 99% of opened tickets resolved on time. |
| 3 | **Recurring Reports Accuracy/Timeliness.** Produce recurring reports (defined as the Weekly Status Reports described in Section 4.3, Recurring Management Reports described in Section 4.5.1) in accordance with approved requirements accurately and on time (defined as due dates in the Project Schedule).  (Any unapproved deviation from timeliness and accuracy standards will be corrected on a schedule based on critical nature of the deviation as determined by the State.) | 100% of reports are accurate and delivered on time. |
| 4 | **Work Product Compliance.** Ensure work products comply with all standards identified in the Contract. (Any unapproved deviation from standards will be corrected within ten (10) calendar days of detection by the Contractor or State). | 100% compliance, unless otherwise approved by the State. |
| 5 | **Security Incident Notification Timeliness.** Security Incidents shall be made known to the FSSA Privacy & Security Office and appointed DFR team (noted in the Project Management Plan) within one (1) hour of when Contractor discovered the Security Incident.  Please see Section 12 of Attachment B for the definitions of “Security Incident”, “discovered”, and “discovery”. | 100% compliance, as measured by time elapsed from Security Incident discovery |
| 6 | **Privacy and Security Compliance.** AS solution and Contractor are compliant with key Federal laws and regulations (e.g. ADA, OSHA, Medicaid, SNAP, TANF, etc.), Indiana Law, MARS-E 2.0 (and subsequent versions), and HIPAA requirements for privacy and security in all activities.  Please see Section 12 of Attachment B for the definition of “breach” and additional relevant information. | No incidents of non-compliance.  (Any incidents of non-compliance discovered by or reported to the State shall be cured by the Contractor within 30 calendar days upon notice by the State; satisfactory failure to cure would subject the Contractor to the Withhold established below and repeated failures to cure would be cause for termination of the agreement.) |

1. **M&O Withhold Amount and Conditions**

During each month of the Contract, the State will withhold 10% of that month’s fees as listed in the contract. The State will evaluate service level noncompliance monthly. If two (2) or more M&O service levels as defined in Section 12.2.1. a. are not reached for any given month, the performance withhold amount for that month will be at risk for forfeit unless all metrics are met in the next two consecutive months. At the State’s request, the Contractor shall perform a Corrective Action Plan (CAP) that outlines how the Contractor plans to correct poor performance.

If two or more instances of failure to meet M&O SLAs (as detailed in above) are reported in two (2) consecutive months, the Contractor must prepare and submit a root-cause analysis and remediation plan to the State, the form and scope of which shall be agreed to by the parties.

1. **Other Service Levels**

The service levels in the table below are established in the Contract but are not included in the determination of whether the 10% performance withhold mentioned above will be released for any given month. Instead, in cases of non-compliance with regards to the service levels in the table below, the Contractor shall perform a Corrective Action Plan (CAP) at the State’s request that outlines how the Contractor shall correct poor performance. The State may also require the Contractor to prepare and submit a root-cause analysis and remediation plan to the State, the form and scope of which shall be agreed to by the parties. If there are multiple instances of non-compliance, the State reserves the right to pursue additional corrective actions or contract termination.

| **SLA#** | **Key Service Level Agreement** | **Threshold for Compliance** |
| --- | --- | --- |
| 7 | Forward all communications received that should be handled by State staff or interface partner staff (as applicable) within one (1) business day of receipt | 100% compliance, unless otherwise approved by the State |
| 8 | Notify the sender that communications have been forwarded to the State or interface partner staff (as applicable) within one (1) business day of receipt | 100% compliance, unless otherwise approved by the State |
| 9 | Propose a replacement of key staff positions within thirty (30) calendar days of vacancy | 100% compliance, unless otherwise approved by the State |
| 10 | Provide monthly management reports within ten (10) calendar days of the end of the month being reported | 100% compliance, unless otherwise approved by the State |
| 11 | Submit status meeting agenda at least one (1) business day prior to meeting | 95% compliance, unless otherwise approved by the State |
| 12 | Provide status meeting minutes in specified format within ten (10) business days of the meeting | 95% compliance, unless otherwise approved by the State |
| 13 | Provide Service Level Agreement status reports in specified format at least one (1) business day prior to each meeting | 100% compliance, unless otherwise approved by the State |
| 14 | Provide annual summary reports in specified format | 100% compliance, unless otherwise approved by the State |
| 15 | Produce accurate documentation within ten (10) days of required change | 100% compliance, unless otherwise approved by the State |
| 16 | Notify the State of any issues with any user or system interface within one (1) hour of detection of the issue | 100% compliance |

* 1. **SDLC Service Levels**
     1. **SDLC Thresholds for Compliance**

The following are service levels for SDLC activities (e.g., defect fixes and enhancements). These will be reported monthly to the State in a written report, per Section 4.5.1.

|  |  |  |
| --- | --- | --- |
| **SLA#** | **Key Service Level Agreement** | **SLA Threshold for Compliance** |
| 17 | **Enhancement Estimates Timeliness.** Provide enhancement cost and time estimates within one (1) week from request submission. | 95% compliance |
| 18 | **Enhancement Completion Timeliness.** Complete requested enhancements within estimated timeframes approved by the State. | 100% compliance |
| 19 | **Defect Correction Timeliness.** Correct defects found during User Acceptance Testing per the timeframes according to the timelines in Section 5.3.5, under UAT Defect Remediation Schedule. The Contractor shall receive State approval on which defect Severity Level 3 and 4 defects are allowed to be uncorrected before production.  See Section 5.3.2 for the Defect Severity level definitions. | Correct 100% of Severity Level 1 and 2 defects and 95% of Severity Level 3 and 4 defects) per the timeframes agreed upon with the State |
| 20 | **Budget Adherence.** The Contractor shall complete requested enhancements within the State-approved budget. The Contractor shall be responsible for any expenditures over the State-approved budget if no changes in scope were made. | 100% compliance |

* + 1. **SDLC Performance-Based Withhold**

During each month of the Contract, the State will withhold 10% of that month’s invoiced SDLC fees (that is, non-M&O fees). The State will evaluate SDLC-related service levels monthly for noncompliance. If two (2) or more service levels as defined in Section 12.3.1 are not reached for any given month, the performance withhold amount for that month will be at risk for forfeit unless all metrics are met in the next two consecutive months. At the State’s request, the Contractor shall perform a Corrective Action Plan (CAP) that outlines how the Contractor shall correct poor performance.

If two (2) or more instances of failure to meet an SLA (as detailed in above) are reported in two (2) consecutive months, Contractor must prepare and submit a root-cause analysis and remediation plan to the State, the form and scope of which shall be agreed to by the parties.

* 1. **User Requests/Defects/Incidents Reporting**

The Contractor will report the number of items (user requests, defects, and incidents) resolved and remaining open items in a given monthly period, the amount of time each item has been open, and the amount of time originally estimated for each item’s resolution.