Performance Work Statement (PWS)

**Department of Labor (DOL) Technology, Innovation and Engineering (TIE) Services**

[PART 1 4](#_Toc183177582)

[General Information 4](#_Toc183177583)

[1.1. Description of Services/Introduction 4](#_Toc183177584)

[1.2. Background 5](#_Toc183177585)

[1.3. Objectives 5](#_Toc183177586)

[1.4. Scope 5](#_Toc183177587)

[1.4.1. Artificial Intelligence Services 5](#_Toc183177588)

[1.4.2. Enterprise Engineering and Architecture 6](#_Toc183177589)

[1.4.3. Mobile App Development 6](#_Toc183177590)

[1.4.4. Emerging Technology 6](#_Toc183177591)

[1.4.5. Security Solutions 7](#_Toc183177592)

[1.4.6. Electronics Records Management 7](#_Toc183177593)

[1.4.7. All Other Solutions 7](#_Toc183177594)

[1.5. Period of Performance 7](#_Toc183177595)

[1.6. General Information 8](#_Toc183177596)

[1.6.1. Quality Control 8](#_Toc183177597)

[1.6.2. Quality Assurance: 8](#_Toc183177598)

[1.6.3. Government Remedies 8](#_Toc183177599)

[1.6.4. Recognized Holidays 8](#_Toc183177600)

[1.6.5. Hours of Operation 9](#_Toc183177601)

[1.6.6. Place of Performance 9](#_Toc183177602)

[1.6.7. Type of Contract 10](#_Toc183177603)

[1.6.8. Security Requirements 10](#_Toc183177604)

[1.7. Special Qualifications 29](#_Toc183177605)

[1.7.1 Key Personnel 29](#_Toc183177606)

[1.7.2 Organizational Conflict of Interest: 39](#_Toc183177607)

[1.7.3 Phase In/Phase Out Period 39](#_Toc183177608)

[Part 2 40](#_Toc183177609)

[Definition & Acronyms 40](#_Toc183177610)

[Part 3 41](#_Toc183177611)

[Government Furnished Property, Equipment, And Services 41](#_Toc183177612)

[3.1 General: 41](#_Toc183177613)

[3.2 Equipment: 41](#_Toc183177614)

[3.3 Facilities: 41](#_Toc183177615)

[Part 4 42](#_Toc183177616)

[Contractor Furnish Items and Services 42](#_Toc183177617)

[4.1 General: 42](#_Toc183177618)

[4.2 Clearance: 42](#_Toc183177619)

[Part 5 43](#_Toc183177620)

[Specific Tasks 43](#_Toc183177621)

[5.1 Services 43](#_Toc183177622)

[Task Area 1: Artificial Intelligence 43](#_Toc183177623)

[Task Area 2: Advanced Engineering 44](#_Toc183177624)

[Task Area 3: Electronics Records Management 44](#_Toc183177625)

[Task Area 4: Emerging Technology 44](#_Toc183177626)

[Task Area 5: Enterprise Architecture 45](#_Toc183177627)

[5.2 Transition-In 46](#_Toc183177628)

[5.3 Program and Project Management 46](#_Toc183177629)

[5.3.1 Task Order Management Plan 48](#_Toc183177630)

[5.3.2 Integrated Project Team (IPT) 48](#_Toc183177631)

[5.3.3 Monthly Progress Report 48](#_Toc183177632)

[5.4 System/Application Development, Operations, and Maintenance 49](#_Toc183177633)

[5.4.1 Operations Support Services 49](#_Toc183177634)

[5.4.2 Maintenance Support Services 50](#_Toc183177635)

[5.4.3 Development and Enhancements 50](#_Toc183177636)

[5.4.5 DevSecOps 50](#_Toc183177637)

[5.4.6 Test Plan & Execution 51](#_Toc183177638)

[5.4.7 Release Management 52](#_Toc183177639)

[5.5 Training 53](#_Toc183177640)

[5.6 Transition-Out 53](#_Toc183177641)

[Part 6 55](#_Toc183177642)

[Applicable Publications 55](#_Toc183177643)

[6.1 Publications Applicable to This PWS: 55](#_Toc183177644)

[6.1.1 Laws (Mandatory) 55](#_Toc183177645)

[6.1.2 Federal Guidance (Mandatory) 56](#_Toc183177646)

[6.1.3 Industry standards (Advisory) 57](#_Toc183177647)

[6.1.4 DOL specific standards, policies, and procedures (Advisory) 57](#_Toc183177648)

[Part 7 58](#_Toc183177649)

[Technical Exhibit Index 58](#_Toc183177650)

[Technical Exhibit 1 59](#_Toc183177651)

[Performance Requirements Summary 59](#_Toc183177652)

[Technical Exhibit 2 64](#_Toc183177653)

[Deliverables Schedule 64](#_Toc183177654)

[Electronic Records Management 66](#_Toc183177655)

[Technical Exhibit 3 66](#_Toc183177656)

[Task Area 1: Artificial Intelligence 66](#_Toc183177657)

[Task Area 2: Enterprise Engineering and Architecture 67](#_Toc183177658)

[Task Area 4: Emerging Technology 68](#_Toc183177659)

[Task Area 6: Electronics Records Management 68](#_Toc183177660)

# PART 1

## General Information

The contractor shall provide personnel to perform services as defined in this Performance Work Statement (PWS) for the US Department of Labor, heretofore known as “the government” in support of Artificial Intelligence (AI) Implementation Services.

## Description of Services/Introduction

The contractor shall provide all personnel, equipment, tools, materials, supervision, and other items and non-personal services necessary to provide Artificial Intelligence Implementation support, Advanced Engineering Integration, Electronics Records Management, Emerging Technology and Enterprise Architecture support services, Mobile Application Development, Security Solutions, and other services as defined in this Performance Work Statement, except as Specified in section 3 as government furnished property and services. The contractor shall perform to the standards in this contract action.

## Background

The Department of Labor (DOL) is a large cabinet level Agency that employs over 16,000 federal staff. Most of DOL’s workforce is spread nationwide in Regional, District, Field, and home offices, which lead to some constraints in IT solutions for an office or an individual DOL Employee. The Office of the Chief Information Officer (OCIO) is a customer service organization dedicated to providing information technology leadership, products and support for the DOL. OCIO plays a critical leadership role in driving reforms to help control system development efforts, better manage technology spending, and succeed in achieving real, measurable improvements in mission performance. The Technology, Innovation and Engineering Directorate (TIE) is responsible for providing and bringing the latest technology and world class services in the areas of Emerging Technology, Artificial Intelligence, Advanced Engineering, Mobile App development, Electronics Records Management, and Security Solutions and promote and bring Innovation to DOL to make improvements in mission performance.

## Objectives

The objective of this requirement is to obtain contractor support for the development, modernization, and enhancement (DME), and Operations and Maintenance (O&M) of Information Technology (IT) services and products for OCIO that support new, integrated, reusable applications/ services/ frameworks as well as build upon existing applications/ services/ frameworks in compliance with all DOL standards (such as: agile, data, security, 508, responsible AI, architecture, development, testing, performance, deployment, infrastructure, and operations). The work output will be in Task Areas such as Artificial Intelligence, Advanced Engineering, Electronics Records Management, Emerging Technology, Enterprise Architecture, Mobile Application Development, Security Solutions, and Other Services as required by DOL that may be cross cutting and span multiple task areas.

## Scope

The contractor will provide DME and O&M services as outlined below:

### 1.4.1. Artificial Intelligence Services

The Artificial Intelligence Services scope is inclusive of, but not limited to (a) Enterprise AI tools (b) AI Models (c) AI Governance, and (d) AI-Ops.

Sample activities include: (a) developing, deploying, enhancing, and maintaining reusable (new or existing) enterprise AI tools, services, and frameworks for DOL wide use; (b) deploying advanced AI models (such as language models, ML), algorithms, and frameworks to enhance business processes of DOL agencies; (c) integrating AI solutions with existing IT infrastructure to provide accurate decision-making insights; (d) providing AI governance support as required; (e) supporting all aspects of AI operations for AI IT systems.

All deliverables must comply with Government security and architecture requirements, ensuring the scalability and effectiveness of AI solutions enterprise-wide.

### 1.4.2. Enterprise Engineering and Architecture

The Enterprise Engineering and Architecture scope is inclusive of, but not limited to activities that support the development and review of policies and processes, engineering projects, and platform infrastructures.

Sample activities include: (a) creating and refining the Enterprise Architecture (EA) Data Model, supporting DOL-wide EA standards and governance, and contributing to IT modernization efforts; (b) providing support for new technology implementation, including testing, infrastructure coordination, and reporting capabilities; (c) coordinating operational methodologies and policy deployment for application identification and management to enhance security and compliance; (d) conducting analysis of alternatives as required on new products, tools, and technologies for the DOL ecosystem with a total cost of ownership and people, process, technology mindset.

### 1.4.3. Mobile App Development

The contractor shall provide services for developing new mobile apps, maintaining existing internal and external OCIO-developed apps, and updating each as needed to meet their users’ evolving requirements while following a disciplined process consistent with Kanban Maturity Model level 3.

### 1.4.4. Emerging Technology

The Emerging Technology scope is inclusive of but not limited to Quantum Computing including activities related to post quantum crypto (PQC) readiness and quantum algorithms, support for innovative technologies such as Augmented Reality & Generative AI, ability to evaluate and bring in new technologies and services to the DOL ecosystem as required by DOL.

Sample activities include: (a) conducting analysis of alternatives and developing proof of concepts on the latest emerging technologies and security practices; (b) identifying innovative approaches and technologies to improve services provided by the DOL; (c) improving processes for all aspects outlined in the objectives such as security and development; (d) conducting technical reviews for all workstreams of TIE and for all objectives outlined above such as architecture, security, etc.; (e) develop and or maintain platforms to support DOL enterprise needs such as for AI and PQC.

The output from these activities must support and improve the DME and O&M within TIE and must ensure that the services offered align with the latest advancements and meet the highest standards of compliance (e.g., security).

### 1.4.5. Security Solutions

The Security Solutions scope is inclusive of, but not limited to implementing and ensuring compliance with security risk management frameworks (such as NIST RMF, NIST AI RMF) and all Office of the Chief AI Office (OCAIO), Chief Technology Officer (CTO), and DOL requirements by implementing tools, solutions, processes, and monitoring.

Sample activities include: (a) performing security reviews of all DME and O&M deliverables within TIE; (b) developing and applying measurable security risk model frameworks for AI and PQC readiness; (c) developing and/or supporting custom developed and/or Commercial Off The Shelf (COTS) productions for managing enterprise security for DOL in areas such as AI and PQC; and (d) leading and supporting all aspects of migration and modernization of all DOL systems (such as applications, services, platforms) for AI and PQC security readiness.

### 1.4.6. Electronics Records Management

The contractor shall provide design, development and implementation support which includes technical and project management support for the DOL Electronics Records Management System (eRMS).

This project is being undertaken to meet federal mandates and in response to a 2017 OIG finding on our current records management practices. Federal mandate OMB Memorandum M-23-07 requires that all federal agencies fully manage all permanent records electronically. In addition, the National Archives and Records Administration (NARA) no longer accepts paper records.

### 1.4.7. All Other Solutions

This task area for the provision of various task order services, encompassing Artificial Intelligence, Advanced Engineering, Electronics Records Management, Emerging Technology, Enterprise Architecture, Mobile Application Development, and Security Solutions. The objective is to enhance operational efficiency, technological advancement, and data that may be required to fulfill DOL OCIO TIE mission and DOL agency requirements.

## Period of Performance

The period of performance shall be for one (1) Base Period of 12 months and four (4) 12-month option periods.

The Period of Performance reads as follows:

Base Period: August 1, 2025 – July 31, 2026

Option Period I: August 1, 2026 – July 31, 2027

Option Period II: August 1, 2027 – July 31, 2028

Option Period III: August 1, 2028 – July 31, 2029

Option Period IV: August 1, 2029 – July 31, 2030

The government reserves the right to extend the term of this contract action at the prices set forth in Section B in accordance with the terms and conditions contained in clause 52.217-9 entitled, “Option to Extend the Term of the Contract”.

## General Information

### 1.6.1. Quality Control

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor’s quality control program is the means by which he assures himself that his work complies with the requirement of the contract. As a minimum, the contractor shall develop quality control procedures that address the areas identified in Technical Exhibit 1, “Performance Requirements Summary”. After acceptance of the quality control plan, the contractor shall receive the Contracting Officer’s acceptance in writing of any proposed change to his QC system. The Contractor shall provide a detailed QCP to the COR within fifteen (15) calendar days of contract award. Revisions to the QCP must be submitted to the COR ten (10) calendar days prior to implementation. At a minimum, the Contractor shall develop quality control procedures that:

* Enable the Contractor to identify and correct deficiencies in the quality of service before task activities occur and/or the Government points out the deficiencies.
* Provide procedures for documenting and responding to Federal questions/queries.

### 1.6.2. Quality Assurance:

The government shall evaluate the contractor’s performance under this contract action in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

### 1.6.3. Government Remedies

The Contracting Officer shall follow FAR 52.212-4, “Contract Terms and Conditions-Commercial Items” or 52.246-4, “Inspection of Services-Fixed Price” for contractor’s failure to perform satisfactory services or failure to correct non-conforming services.

### 1.6.4. Recognized Holidays

New Year’s Day Labor Day

Martin Luther King Jr.’s Birthday Columbus Day

President’s Day Veteran’s Day

Memorial Day Thanksgiving Day

Juneteenth Day Christmas Day

Independence Day

Presidential Inauguration Day: Most Federal offices in the District of Columbia/Maryland/Virginia (DMV) metropolitan area are closed on the day a President is inaugurated on January 20th for each fourth year after 1965 (see 5 U.S.C. 6103(c)).

Any of the above holidays falling on a Saturday or Sunday shall be observed on the date designated by the Federal Government. Observance of such days by Government personnel shall not be cause for additional period of performance or entitlement to compensation except as set forth in the contract. If the contractor’s personnel work on a holiday, the Government will not reimburse the contractor for holiday or other premium compensation unless authorized pursuant to an overtime clause elsewhere in the contract.

When the Government grants administrative leave to its Government employees for reasons such as inclement weather, unanticipated holidays declared by the President, or similar reasons, the contractor shall also dismiss assigned contractor personnel working on-site unless prohibited elsewhere in the contract. However, the contractor agrees to continue to provide sufficient personnel to perform the requirements of critical tasks already in operation or scheduled, and if necessary, shall seek guidance from the contracting officer or his/her duly authorized representative pertaining to such requirements. If work is being performed under a labor-hour or time-and-materials order, reimbursement will only be made on the basis of time worked.

Inclement Weather and/or Other Conditions Which Affect Building Closures:

Contractor support is not required in the event of a government closure unless specifically required in the Order award. In cases such as these, the Contractor may work during periods of time when segments (buildings or business) of DOL are closed for any reason, provided security measures are followed. Such times may include Agency, and facility closures due to inclement weather, late openings, early dismissals, building closures, or legal holidays.

### 1.6.5. Hours of Operation

The contractor is responsible for conducting performance between the hours of 6:00 am to 8:00 pm eastern, Monday thru Friday, except Federal holidays or when the government facility is closed due to local or national emergencies, administrative closings, or similar government directed facility closings. The contractor must at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this statement of work when the government facility is not closed for the above reasons. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the work force are essential.

### 1.6.6. Place of Performance

The work to be performed under this contract action will be performed at the contractor’s facility or remotely.

The Government will not provide or reimburse contractor employees for internet connectivity.

Regardless of location, Contractor employees must employ appropriate safeguards and comply with any and all applicable DOL and Federal polices, specification/requirements, and procedures related to Personally Identifiable Information (PII), security, network, data, and communications.

The Contractor shall limit work performed under this resulting Contract to locations within the continental United States (lower 48 states and Washington, DC).

The Contractor is not required to travel during the performance of this contract.

### 1.6.7. Type of Contract

The government anticipates award of a Labor Hours (LH) and/or Firm Fixed Price contract.

### 1.6.8. Security Requirements

Applications provided by the vendor for use by the government are fully functional and operate correctly as intended on systems using the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology’s website at [http://checklists.nist.gov](http://checklists.nist.gov/).

Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

No hardware, software, or service provided by the vendor may use or incorporate any hardware, software, or services developed or provided by Kaspersky Lab.

No hardware, software, or service provided by the vendor may use or incorporate any equipment, system, or service that uses covered telecommunications equipment or services (as defined in FAR Subpart 4.21) as a substantial or essential component of any system, or as critical technology as part of any system.

The vendor shall incorporate a Supply Chain Risk Management (SCRM) process for any hardware or software provided to the government.  The vendor shall provide a description of this SCRM process to the government prior to delivery of the hardware/software. For example: <https://www.fbi.gov/file-repository/scrmbestpractices-1.pdf/view>

As determined applicable by the Government, the Vendor agrees to comply with the following statutes, regulations, standards, and policies:

* + Federal Information Security Modernization Act (FISMA) of 2014
  + Title III of the E-Government Act of 2002—Federal Information Security Management Act (FISMA), as amended.
  + Homeland Security Presidential Directive 12 “Policy for a Common Identification Standard for Federal Employees and vendors”
  + The Computer Security Act of 1987
  + Office of Management and Budget (OMB) Circulars and Memorandums (i.e., A-130, Appendix III, Security of Federal Automated Information Resource)
  + Federal Information Processing Standard (FIPS) 140
  + Federal Information Processing Standard (FIPS) 199
  + Federal Information Processing Standard (FIPS) 200
  + National Institute of Standards and Technology (NIST) Special Publications (SP) Series
  + Executive Order 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government
  + Executive Order 14110 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
  + OMB M-24-10 Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence
  + OMB M-24-18 Advancing the Responsible Acquisition of Artificial Intelligence in Government
  + Trusted Internet Connections (TIC) initiative (Update), (M-09-32), September 17, 2009
  + The Privacy Act of 1974, 5 U.S.C. § 552a, as amended
  + The Freedom of Information Act, PL 93-502 And other DOL-specific security regulations and policies, such as:
* Department of Labor (DOL) Computer Security Handbook (CSH)
* DOL Manual Series (DLMS) 9 – 400, IT Security
* DLMS 0 – 1200, DOL Safeguarding Sensitive Data Including Personally Identifiable Information
* Portable Systems Equipment Policy

Depending on the types and extent of access to data and systems required for the work, vendor personnel may be required to undergo a background investigation and obtain a security clearance.  The vendor shall ensure any requirements and submissions are completed within the timeframe requested by the government.

DOL reserves the right to review and approve or disapprove all the security safeguards instituted to comply with the requirements of this contract.

If the Vendor fails to comply with the cybersecurity and privacy requirements, the Vendor shall be deemed to have failed to perform the provision of this contract.

Vendor must include the Government’s cybersecurity and privacy provisions contained in this contract in every solicitation and every subcontract associated with the work performed under this contract.

**​1.6.8.1 Badging**

All Vendor employees selected to work under this contract with an appointment over six months must be issued a Personnel Identity Verification (PIV) card in accordance with Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Vendors.

a) Consult with the COR to determine the level of security required for Vendor employees.

b) Ensure the Vendor has all required documents and approvals from the COR.

c) Arrange with the COR for the date, time, and location for PIV processing.

d) Ensure that Vendor employees report, with all required documents, to the reporting location determined by the COR.

Upon submission of required PIV documents, Vendor employees will be granted temporary access.  If the required forms are not submitted, no access will be granted and no claim against the Government will occur.

**Account Issuance**: If any contract employees must be issued DOL Local Area Network (LAN) IDs, then each such employee must agree to abide by DOL network “Rules of Behavior” prior to receiving an ID.  In addition, staff who are issued LAN IDs will need to follow DOL separation procedures.  These procedures will be provided to the Vendor through the COR.  The Vendor will assume responsibility that these procedures are followed.

**Training**: Where required and applicable, vendor employees, including employees of sub-vendors at any tier, shall complete any DOL designated and hosted training, that the Contracting Officer's Representative (COR) identifies as mandatory. Training shall be completed in a timeframe specified by the COR.

Time spent on training shall be counted as regular hours worked.

**1.6.8.2 Application Development Security**

I. GENERAL

The Vendor shall agree to maximize the security of the software development throughout the term of this Contract according to general industry standards including but not be limited to the following terms and conditions.

The Contract shall clarify the security-related rights and obligations of all the parties to a software development relationship including any third-party vendors, subcontractors or other entities hired by Vendor.

The Vendor shall agree in writing that the terms of this Contract shall apply to Vendor's employees, as well as to third party vendors and subcontractors that will be employed by Vendor for the Contract.

The Vendor shall take all actions necessary to protect information regarding security issues and associated documentation, to help limit the likelihood that vulnerabilities in operational Government software are exposed.

Consistent with the provisions of this Contract, the Vendor shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. The "highest applicable industry standards" shall be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

1. **Personnel**

The Vendor shall identify in writing the person who will be responsible for overall security of the application development, management, and update process throughout the Contract period. The person identified shall be a single senior technical security specialist, to be known as the project Security Lead.

The Security Lead shall certify in writing the security of each deliverable.

1. **Security Training**

The Vendor shall be responsible for verifying that all members of the developer team have been successfully trained in secure programming techniques.

The Vendor shall document the process including training courses that their application developers have taken prior to developing applications under this Contract.

The Vendor shall certify to the Government that only application developers who have received appropriate level of formal training on secure application development and passed a competency test on application security shall be involved in the Contract.

**(c) Background Checks of Developers**

The vendor shall perform appropriate background investigations of all development team members and shall certify that all individuals who will be involved in this Contract and the software development process have cleared the background investigation.

1. **Vulnerabilities, Risks and Threats**

The Vendor shall agree in writing that they will strive to identify vulnerabilities, risks and threats as early as possible at any time during the software lifecycle. The software lifecycle shall mean from development, management, and updates through retirement of such application.

The Vendor shall identify the key risks to the important assets and functions provided by the application. The Vendor shall conduct an analysis against an industry-recognized list of common programming errors – such as the [*SANS Top 25 Most Dangerous Programming Errors*](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.sans.org%2Ftop25-software-errors%2F&data=04%7C01%7CPickett.Ebony.2%40DOL.gov%7C5718fe6ffb90447de50808d9d14a7f4c%7C75a6305472044e0c9126adab971d4aca%7C0%7C0%7C637770940163792941%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=0z1u3h5sEGcGg8591lQRg2KX3uLG7rJNtG6hpqZfcqc%3D&reserved=0)*–*current security risk and vulnerabilities – such as *Open Web Application Security Project (OWASP Top Ten), 2020 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses* – and document in writing that they have been mitigated. The Vendor shall conduct risk assessment(s) to determine and prioritize risks, enumerate vulnerabilities, and understand the impact that particular attacks might have on an application to ensure it meets applicable contractual obligations, regulatory mandates and security best practices and standards.

The Vendor shall share with the Government in writing all security-relevant information regarding the vulnerabilities, risks and threats to the application immediately and completely upon identification. Such security documentation shall describe security design, risk analysis, or issues.

**(e) Application Development**

The Vendor shall provide the Government written documentation detailing their application development, patch management, and update processes. The documentation shall clearly identify the measures that will be taken at each level of the process to develop, maintain and manage the software securely.

The Vendor shall provide secure configuration guidelines in writing to the Government that fully describe all security relevant configuration options and their implications for the overall security of the software. The guideline shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security. The default configuration of the software shall be secure.

The Vendor shall follow NIST Special Publication 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations” and SP800-64 Rev. 2 “Security Considerations in the System Development Life Cycle” in the application software lifecycle.

Applications provided by the vendor for use by the government are fully functional and operate correctly as intended on systems using the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology’s website at <http://checklists.nist.gov>.

Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

The Vendor shall specify in writing to the Government what additional industry security standards and level of care that they follow.

The Vendor shall agree in writing to comply with such standards and level of care. The Vendor shall provide written documentation to the Government that clearly explains the design for achieving each of the security requirements. The Vendor shall provide and follow a set of secure coding guidelines. These guidelines will indicate how code should be formatted, structured, and commented. All security-relevant code shall be thoroughly commented. Specific guidance on avoiding common security vulnerabilities shall be included. Also, all code shall be reviewed by at least one other Developer against the security requirements and coding guideline before it is considered ready for test.

The vendor shall agree in writing to work with the government to identify early in the system development life cycle, the functions, ports, protocols, and services intended for use.  This includes systems that provide external services as well as internal systems.

The vendor must state in writing to the government that IT products that use PIV capable technologies are on the FIPS 201-approved list for Personal Identity Verification (PIV).

II. DEVELOPMENT ENVIRONMENT

**(a) Secure Coding**

The Vendor shall disclose what tools are used in the software development environment to encourage secure coding.

**(b) Configuration Management**

The Vendor shall use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

**(c) Distribution**

The Vendor shall use a build process that reliably builds a complete distribution from source. This process shall include a method for verifying the integrity of the software delivered to the Government.

**(d) Disclosure**

The Vendor shall document in writing to the Government all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

**(e) Evaluation**

The Vendor shall make reasonable efforts to ensure that third party software meets all the terms of this agreement and is as secure as custom developed code developed under this agreement.

III. TESTING

**(a) General**

The Vendor shall provide and follow a security test plan that defines an approach for testing or otherwise establishing that each of the security requirements has been met. The level of rigor of this test process shall be detailed in the plan. The vendor shall implement the security test plan and provide the test results to the Government in writing.

**(b) Source Code**

The Vendor shall agree in writing to the Government that during the application development lifecycle process the source code shall be evaluated to ensure the requirements of this Contract including the security standards, policies and best practices are followed. The Vendor shall have a well-documented procedure and framework for conducting code reviews.

The Vendor shall conduct static and dynamic code analysis throughout the lifecycle as directed to ensure flaws are mitigated prior to delivery, execution. The results to include before and after mitigations shall be provided.

**(c) Vulnerability and a Penetration Test**

The Vendor shall agree in writing that prior to production the application shall undergo vulnerability and a penetration test.

Postproduction, the Vendor shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase.

The Vendor shall provide to the Government written documentation of the results of the scans and tests along with a mitigation plan.

The Vendor shall agree in writing that these vulnerabilities shall be mitigated within a pre-negotiated period.

**(d) Patches and Updates**

The Vendor shall provide notification of patches and updates affecting security within a pre-negotiated period as identified in the patch management process throughout the software lifecycle.

The Vendor shall apply, test, and validate the appropriate patches and updates and/or workarounds on a test version of the application before distribution.

The Vendor shall verify and provide written documentation that all updates have been tested and, prior to production, installed.

The Vendor shall verify application functionality, based upon pre-negotiated procedures, at the conclusion of patch updates, and provide documentation of the results.

**(e) Tracking Security Issues**

The Vendor shall track all security issues uncovered during the entire software lifecycle, whether a requirements, design, implementation, testing, deployment, or operational issue. The risk associated with each security issue shall be evaluated, documented, and reported to Government as soon as possible after discovery.

IV. DELIVERY OF THE SECURE APPLICATION

The Vendor shall provide a "certification package" consisting of the security documentation created throughout the development process. The package shall establish that the security requirements, design, implementation, and test results were properly completed, and all security issues were resolved appropriately.

The Vendor shall resolve all security issues that are identified before delivery. Security issues discovered after delivery shall be handled in the same manner as other bugs and issues as specified in this Agreement.

1. **Self-Certification**

The Security Lead shall certify to the Government in writing that the software meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status shall be fully documented with the delivery.

1. **No Malicious Code**

Developer warrants that the software shall not contain any code that does not support a software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

V. SECURITY ACCEPTANCE AND MAINTENANCE

1. **Acceptance**

The software shall not be considered accepted until the Vendor certification package is complete, and all security issues have been resolved.

1. **Investigating Security Issues**

After acceptance, if security issues are discovered or reasonably suspected, Vendor shall assist the Government in performing an investigation to determine the nature of the issue.

The Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies. DOL reserves the right to levy additional security requirements if new or unforeseen risks are discovered at a future time or if new security policies are mandated on Government agencies.

**1.6.8.3 Security and Privacy Requirements**

Vendor staff are required to conform to all applicable sections of the U.S. Code and the Code of Federal Regulations (CFR) and DOL’s security and privacy policies.

The sections below highlight key areas of compliance required by the Vendor staff and its subcontractors.

Compliance with the Federal Regulations and Laws: Program systems shall be subject to security reviews, as required by the Government before and throughout the period of performance. In the event the program/system is identified for a review, the Vendor shall assist TIE in providing support upon request during the DOL Inspector General (IG) or other federally supported IG audit processes (i.e., providing supporting evidence, ad-hoc reports, interviews, documentation, etc.).

Where the Vendor is required custody of sensitive information under this contract, it must be protected under the Privacy Act of 1974, 5 U.S.C. § 552a – as Amended. The Offeror shall be responsible for safeguarding Personally Identifiable Information (PII) against unauthorized disclosure, dissemination, or modification in accordance with contract requirements, law, and DOL PII policy and regulations. This shall include but is not limited to Privacy and PII data located in IT systems, software, research data/information, documentation, personnel (institutional knowledge) and facilities.

The Vendor shall immediately notify the TIE COR and the DOL Information Security Officer (ISO) when a security incident(s) is suspected or verifiably detected, so the other parties may take steps to determine whether there has been a compromise and to take appropriate security precautions. Vendor staff will provide reasonable support in analysis and /or investigation into any security incidents.

In the event of a disruption, the Vendor shall immediately (within 15 minutes of discovery) notify the COR that a disruption has occurred and describe the contingency operations undertaken or to be undertaken to avoid a disruption of services.

The Vendor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of 18 US Code Section (USC) 641 (Criminal Code: Public Money, Property or Records).

**1.6.8.4 Physical Security**

The Vendor shall be responsible for ensuring compliance by its employees and subcontractors with physical security requirements of DOL and other Government installations or Vendor facilities where work is performed under this support contract. This includes the safekeeping and display of a DOL-issued photo ID badge for Vendor personnel and any subcontractors while these employees are in federally owned or leased property. The Vendor shall ensure the security of all physical DOL property, building ID badges, key cards and standard keys issued to the Vendor staff. The Vendor shall ensure that employees leaving this support contract permanently or for an extended period of time must return badges, property, key cards, parking place cards, and key the same day the employee leaves.

The Vendor shall control access to its facilities, equipment, material and documents by employees and visitors via electronic and/or physical methods corresponding to the sensitive nature of the work being performed, and information being handled. Electronic and physical methods of security include, but are not limited to, guards, intrusion detection devices, surveillance cameras, lighting, and fencing. For a complete reference of recommended physical security controls, please refer to NIST Special Publication 800-53.

1. **Personnel Security:**

DOL’s work environment is considered sensitive but unclassified. DOL is required under the Homeland Security Presidential Directive (HSPD-12) “Policy for Common Identification Standard for Federal Employees and Vendors” to perform a Minimum Background Investigation (MBI) for Vendors. The MBI is a background investigation that is conducted through the Office of Personnel Management. It is initiated by completing the Standard Government Forms and includes written inquiries to current and past employers, schools, references, and local law enforcement agencies covering the past five years. This investigation will be conducted for the Vendor and Subcontractor staff assigned to perform under this support contract and must have acceptable results. The use of any form other than the Standard Government Forms will not be accepted.

In order to determine personnel suitability, the Vendor/Offeror shall perform, at no cost to the Government, a National Agency Check and Inquiries (NACI) for all personnel proposed to perform any work under this contract. The results of each NACI shall be provided to the CO or COR for review. The CO or COR will make a determination whether to proceed or not with the proposed staff.

Vendor staff shall be required to provide two forms of acceptable identification as described in the Form I-9 Employment Eligibility Verification, provide a current photograph, and be fingerprinted. Successful clearance is required for an employee to continue working under this Contract per Personnel Identity Verification of Vendor Personnel clause of the Federal Acquisition Regulation (FAR).

1. **Personal Identity Verification:**

The Vendor shall comply with DOL personal identity verification procedures as described in the HSPD-12, OMB guidance M-05-4, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

1. **Required Security Training:**

All DOL employees and Vendors must receive security awareness training prior to being given access to DOL systems and periodically thereafter as required by DOL security policies. The Vendor shall ensure that all required training for staff is completed within the designated time frames that are promulgated for the course/topic. Topics include, but are not limited to:

* General Security Awareness Training,
* Safeguarding Personally Identifiable Information, and
* Continuity Awareness
* Role based training for staff with security responsibilities and elevated privileges.

1. **DOL-Specific Security and Privacy Requirements:**

Vendor staff is required to conform to DOL’s security and privacy requirements as described below:

1. **Compliance with the Computer Security Act:**

The Vendor shall comply with the Computer Security Act of 1987. All products and deliverables and services developed or provided under this contract shall comply with the DOL Computer Security guidelines and guidelines contained in Office of Management and Budget (OMB) Circular A-130. All contract staff working in DOL office space, using DOL LAN/WAN and/or accessing DOL computer resources to perform duties under this contract shall agree and sign DOL Rules of Behavior for Computer User and Non-Disclosure Agreements. The Vendor shall submit a copy of each signed and witnessed Non-Disclosure Agreement to the DOL COR prior to the employee performing any work.

1. **Additional Requirements and Provisions:**

The Vendor shall assume all responsibility for creating and submitting the documentation required prior to obtaining access to DOL computer and communication networks for its staff and its subcontractor personnel. DOL will not pay for Vendor’s time spend filling out, submitting, and fixing DOL network access applications. DOL will not reimburse the Vendor for time spent submitting, updating, and managing rejected applications.

The Vendor shall be fully responsible for obtaining and maintaining security accreditation of its facilities and tools, if applicable. Vendor shall have qualified personnel to start execution for transition activities on the day of the kick-off meeting.

**1.6.8.5 Key Control**

The Vendor shall establish and implement methods of making sure all Keys/key cards, if issued to the Vendor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Vendor by the Government shall be duplicated. The Vendor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Vendor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

**1.6.8.5.1 Lost Keys**

In the event keys, other than master keys, are lost or duplicated, the Vendor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the Government, the total cost of re-keying or the replacement of the lock, performs the replacement of locks or rekeying or locks shall be deducted from the monthly payment due the Vendor. In the event a master key is lost or duplicated, the Government and the total shall replace all locks and keys for that system cost deducted from the monthly payment due the Vendor.

**1.6.8.5.1.2 Key Use**

The Vendor shall prohibit the use of Government issued keys/key cards by any persons other than the Vendor’s employees. The Vendor shall prohibit the opening of locked areas by Vendor employees to permit entrance of persons other than Vendor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

**1.6.8.1.3 Lock Combinations**

The Vendor shall establish and implement methods of ensuring that not all lock combinations are revealed to unauthorized persons, if provided. The Vendor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Vendor’s Quality Control Plan.

**1.6.8.1.4 Conservation of Utilities**

The vendor shall instruct employees in utilities conservation practices. The vendor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

**1.6.9 Section Compliance**

**Section 508 Background**

Electronic and Information Technology (EIT)/Information and Communication Technology (ICT) greatly affects how federal agencies, and their employees achieve agency goals, do their daily work and serve the American people. EIT/ICT is also a major gateway to employment opportunities in both the public and private sectors, and it is key to how information is shared with employees, how employees are productive in the workplace, and how they advance in their careers.

**General Requirements**

All EIT/ICT deliverables produced by the VENDOR shall be accessible, usable by assistive technologies, and meet the baseline criteria outlined in Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) August 7, 1998, the Web Content Accessibility Guidelines 2.0 (WCAG 2.0) Level AA and the Department of Labor Management Series (DLMS) Section 9, Chapter 600. EIT/ICT deliverables include but are not limited to websites, software, mobile applications, webcasts, webinars, multimedia (e.g., charts, graphs, graphics, videos, audio tracks, and animation), social media, collaborative workspaces and tools, documents (e.g., PDF, PowerPoint, Excel, and Word), forms and field elements, data tables, image maps, and any training and related training materials.

The Contractor is required to provide ICT that is accessible to people with disabilities, in full conformance with Section 508. The contractor shall ensure that its ICT – including all documentation (project artifacts, system documentation, deployment instructions, user guides, training materials, reports, etc) – allow Federal employees and members of the public with disabilities access and use of information and data that is comparable to the access afforded Federal employees and members of the public who are not individuals with disabilities. More detailed requirements for accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) are provided in Appendix B.

Print materials must be made available in an alternate accessible format when requested. By submitting deliverables pursuant to this contract, VENDOR is certifying that such deliverables are conformant with the accessibility guidelines referenced above.

**Acceptance and Conformance**

By submitting deliverables pursuant to this contract, Vendor is certifying that such deliverables are conformant with the accessibility guidelines referenced above. The Vendor shall include certification of conformance to accessibility standards with all deliverables, and such certification shall be in the form and format defined by the COR. Proof of adequate accessibility, including design, development, and testing data shall be provided to the COR upon request.

Acceptance of deliverables by the Government does not constitute agreement that the deliverables are conformant, and the Government reserves the right to evaluate such deliverables within a reasonable time to assess the Vendor’s certification of accessibility and conformance. Government evaluations, when conducted, will utilize unified test approaches, when applicable, or other appropriate testing methodologies approved by the DOL Section 508 Program Office. Deliverables that are found to be non-conformant will be remediated by the Vendor within a reasonable time and at no additional cost to the Government.

**Accessibility Requirements for Deliverables**

Accessible Formats

All documents and deliverables prepared for or provided to the Government must be in accessible formats (as indicated in the next paragraph). All materials submitted in hardcopy must be provided in an accessible electronic copy at the same time of hard copy submission or alternate accessible format when requested. Any multimedia must include synchronized captions that include all relevant audible information (dialog and sounds), include audio descriptions (when relevant visual information is not otherwise relayed audibly), and be navigable by assistive technologies. Any multimedia interactive interface elements (e.g., user controls) must be navigable by assistive technology and include proper name, role, and/or state properties. Audio-only content shall be accompanied by an accessible screen text or transcript that is an accurate and complete representation of that audio content. The contrast ratio between all content background and foreground colors shall be at least 4.5:1.

All pages within PDFs created for or provided to the Government (to include those created from scanned documents) must be accessible, the content within must be tagged correctly, and must return no potential errors in the Adobe Acrobat Pro’s Accessibility Full Check “Accessibility Report” when tested against the “Adobe PDF” checking option and all of its tests. All graphics, charts, and graphs marked as images/figures within a PDF must be tagged with appropriate, descriptive alternate text conveying equivalent meaning. All text content in the PDF must be readable with assistive technology (e.g., JAWS screen reader) on each page in a comprehensive and sequential manner, to include all information provided in any alternate text descriptions for graphics. Tag order of content (found in the Adobe Acrobat Pro “Navigation Pane”) must match the Reading Order (found in the Adobe Acrobat Pro “Order Pane”) of content through manual verification. Tables shall be tagged properly including column headers, row headers, and assigned scope. Decorative elements that convey no meaning should be marked as Artifacts. Any fillable form fields and buttons must have appropriate form tags, associated tooltips conveying all information needed to correctly complete the field, have a tab order that matches the visual reading order, and be accessible and usable by keyboard only and other assistive technology.

All training, vocal presentations, and training documents must be provided in accessible Section 508 compliant format. “Point-and-click” methods of training with screenshots primarily designed for sighted users is not sufficient. Any screenshots of user actions must be given an equivalent alternate verbal and/or text description and a non-mouse-based action alternative interaction method. All training and reference materials must be provided in an accessible Section 508 electronic format (preferably PDF or Word).

Applicability of Standards

The Section 508 Standards described herein provide the minimum Government requirements and do not, in any way, diminish the vendor’s responsibility to meet additional requirements that may be applicable under the law.

Additional information about accessibility standards related to Section 508 may be found at: <http://section508.gov/>

Additional information about creating accessible PDF files may be found at: <http://www.section508.gov/docs/pdfguidanceforgovernment.pdf>

Requirements for accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) are determined to be relevant. Information about the Section 508 Electronic and Information Technology (EIT) Accessibility Standards may be obtained via the Web at the following URL: http://www.Section 508.gov. Ongoing testing and evaluation shall be done in accordance with the Department of Homeland Security’s (DHS) Trusted Tester Program (<https://www.dhs.gov/trusted-tester>) or equivalent.

**1.6.10 Non-Disclosure Agreements**

All Vendor personnel working on tasks on this effort will be required to sign a formal non-disclosure and/or conflict of interest agreement to guarantee the protection and integrity of government information and documents.

**1.6.11 Post Award Conference/Periodic Progress Meetings**

The Vendor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the vendor to review the vendor's performance. At these meetings, the contracting officer will apprise the vendor of how the government views the vendor's performance and the vendor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

**1.6.12 Contracting Officer Representative (COR)**

A COR will be delegated under a separate cover.

**1.6.13 Contract Manager**

The vendor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the vendor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the vendor on all contract matters relating to daily operation of this contract.

**1.6.14 Identification of Vendor Employees**

All contract personnel attending meetings, answering Government telephones, and working in other situations where their vendor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by vendors are suitably marked as vendor products or that vendor participation is appropriately disclosed. The vendor personnel are required to obtain and wear badges during working hours in the performance of this service.

**1.6.15 Procurement Standards for AI Systems and Services:**

**1.6.15.1 Artificial Intelligence (AI) Definition**

**Artificial Intelligence (AI):** The term “artificial intelligence” has the meaning established in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019,39 which states that “the term ‘artificial intelligence’ includes the following”:

* Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
* An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
* An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
* A set of techniques, including machine learning, that is designed to approximate a cognitive task.
* An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Additionally, the following technical context provided in Section 6 of OMB Memorandum M-24-10 should guide the interpretation of the definition above:

1. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including deep learning, as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
2. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.
3. For this definition, no system should be considered too simple to qualify as a covered AI system due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).
4. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

**1.6.15.2 AI System Development and Usage Requirements**

Pursuant to Executive Orders 13960 and 14110 and guidance issued by the Office of Management and Budget (OMB) 24-10 and 24-18, Federal agencies and contractors are required to report the use of any AI systems that conduct or enhance government business. Furthermore, agencies and contractors must ensure that AI systems are used in a safe a secure manner.

**1.6.15.2.1 Use Case Approval and Tracking**

Contractors that intend to use AI tools to perform contract tasks and/or produce contract deliverables must disclose the use of such tools as part of their proposal. Contractors requiring use of AI systems to perform contract work must identify the product being used and submit that tool for agency approval. For AI systems in use outside of DOL the contractor must implement the respective system security controls as detailed in section 1.6.9 of this PWS.

**1.6.15.2.2 AI Impact Assessments and Responsible AI Review**

At a minimum, the contractor must complete and submit an AI impact assessment that includes the intended purpose for the AI, expected benefits, potential risks, risk mitigation strategies, data quality, and any potential impact on equity and fairness.

Where applicable, contractors are required to submit their AI solution – including unmodified, commercial off the shelf products – for a full Responsible AI Assessment conducted by the agency.

**1.6.15.2.3 AI Model Card Requirements**

Contractors must create and submit a Model Card for each custom-developed AI tool, custom models, and Large Language Models (LLMs)/ Foundational Models supplemented by Retrieval Augmented Generation or otherwise tuned using supplemental data sources

**1.6.15.2.4 AI System Testing Requirements**

Contractors must test all AI solutions for performance in a real-world context to avoid over-fitting to known test data.

**1.6.15.2.5 AI Model Development**

Unless otherwise specified in Part 5 of this PWS, the contractor must ensure that any AI model recommended under this procurement works across multiple cloud environments.

**1.6.15.2.6 AI System Monitoring**

All AI solutions require a plan for conducting ongoing monitoring of those systems. Results of that testing and any subsequent development or tuning conducted to correct for model drift must be fully documented and provided to the agency on a routine basis. Specific deliverables are listed and described in the deliverable’s matrix (Technical Exhibit 2).

**1.6.15.3 Data Handling in AI Systems**

In addition to system and data security controls as detailed in section 1.6.9 of this PWS, Contractors must fully assess and document any data used to help develop, test, or maintain AI applications, regardless of source.

**1.6.15.3.1 Data Assessment Requirements**

The assessment must include the key areas of data quality, representativeness, and bias. The contractor must submit and maintain a plan that outlines and fully documents data collection and curation as it relates to the development, training, testing, and maintenance of all AI tools and systems.

**1.6.15.3.2 Data Interoperability and Access**

Pursuant to OMB memo M-24-10, where practicable, agencies are required to proactively share their custom-developed code, including models and model weights, for AI systems actively in use. Therefore, when possible, it is crucial that contractors avoid the use of proprietary data sets, sensitive government information, or personally identifiable information (PII) in developing and training models to mitigate the risk of unintended disclosure of data from the model. All models require a full model-specific risk analysis.

**1.6.15.4 Additional Requirements for Safety and Rights Impacting AI Tools**

For all contract tasks or deliverables considered to be either safety-impacting or rights-impacting, the contractor must implement additional risk management practices when employing an AI solution.

**1.6.15.4.1 Data Considerations**

Contractors must fully identify, assess, and document the AI system’s impact on equity and fairness, and mitigate algorithmic discrimination when it is present.

**1.6.15.4.2 Consultation and Feedback**

When required, the contractor must assist the agency in the consultation and collection of feedback from affected communities and the public. Such feedback must be considered in the development and maintenance of the AI system or model.

**1.6.15.4.3 Discrimination Monitoring and Remediation**

In addition to conducting ongoing monitoring of AI system performance, the contractor must maintain human consideration and remedy processes to mitigate any discrimination caused using the AI system or tool. The contractor’s plan must include strategies to assist the agency in notifying any negatively affected individuals as well options for individuals to opt-out of AI-enabled decisions as required in M-24-10.

**1.6.15.5 Use of Open-Source and Commercial AI Systems and Services**

Contractors may only use AI products and services in which Government data is protected from unauthorized disclosure and such data is not used to train or otherwise improve the functionality of a specific vendor’s commercial offering and/or any open-source model.

**1.6.15.5.1 Prohibition on Public Model Usage**

Contractors are expressly prohibited from entering either proprietary DOL data or personally identifiable information (PII) into any public AI. This includes the usage of both Large Language Models (LLMs) and Foundational Models in public instances.

**1.6.15.5.2 Appropriate use of Generative AI Resources**

Contractors requiring use of generative AI must identify the specific product and use-case for agency approval. Should the contractor choose to deploy and operate an Open-Source or commercial foundational model or LLM within their own environment, the contractor must implement the respective system security controls as detailed in section 1.6.9 of this PWS.

**1.6.15.5.3 Generative AI Impact, Review, and Disclosure Requirements**

The contractor must complete and submit an AI impact assessment that includes the intended purpose for the Generative AI, expected benefits, potential risks, risk mitigation strategies, quality review processes, and any potential impact on equity and fairness. Where applicable, contractors are required to submit their AI solution for a full Responsible AI Assessment conducted by the agency.

When using any generative AI resource, contractors must fact-check all generative AI responses. This includes but is not limited to reviewing any text, predictions, code, or other output from AI systems thoroughly before adapting or using the output for any official or unofficial documentation. Contractors must ensure any AI results comply with all DOL policies and guidelines, as well as wider federal ethics and safety standards. This review process must be well documented and appear in the contractor’s quality assurance plan.

Contractors must always disclose when generative AI applications have been used to assist in the creation of a work product via footnote or another notation that is clear to the reader/recipient.

**1.6.15.5.4 Generative AI Code Generation and Review Requirements**

To promote efficiency, DOL expects the contractor to use DOL-provided secure AI code development and code generation tools to produce up to 50% of the code required under this contract.

The code generated by the AI tool must follow all quality check procedures recommended for systems development. Contractors will be granted access to available private, DOL instances of generative AI resources on a case-by-case basis.

When using any generative AI resource or LLM, contractors must avoid posting highly sensitive data for processing within any generative AI model. This is especially true when using generative AI models that review software code. Users are expressly prohibited from using generative AI services to review software code that contains restricted information embedded in that code including software keys or other system credentials.

## Special Qualifications

The contractor is responsible for ensuring all employees possess and maintain all required certifications used in the execution of this contract action.

The personnel listed below are considered essential to the work being performed hereunder. Prior to substituting, removing, and replacing any of the key personnel, the Contractor shall notify the Contracting Officer 10 working days in advance and shall submit a written request and justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on this Contract. The proposed substitution of personnel must meet or exceed the education, experience, and other technical requirements of the personnel being replaced and position must be filled within 14 days of being vacated. No change in personnel shall be made by the Contractor without the prior written consent of the Contracting Officer. Resumes of proposed replacement must be provided to the Government for review. The Government must approve the replacement candidate in writing before he/she can start work.

However, in urgent situations, as determined or agreed to by the Contracting Officer, an oral request to substitute key personnel may be approved and subsequently ratified by the Contracting Officer in writing. Such ratification shall constitute the consent of the Contracting Officer required by this paragraph. The Contracting Officer will notify the Contractor within 10 working days after receipt of all required information of the decision on the substitution(s). In the event the proposed substitution of key personnel does not meet or exceed the education, experience, and other technical requirements of the personnel being replaced, the Government reserves the right to require continued performance of previously approved key personnel or to require substitution of acceptable replacements for the individuals specified below. The key personnel listed below may be amended from time to time during the Contract to either add or delete personnel as appropriate.

Key personnel must be available to the Government whenever any work under this contract is being performed. The key personnel shall be available during Core Hours. Core Hours are 10:00 am to 3:30 pm Eastern Time, Monday through Friday, with the exception of Federal Government holidays.

All contractor personnel that are performing development under this PWS must have appropriate experience, credentials, and certifications in related technologies.

### 1.7.1 Key Personnel

The key personnel will vary from task order to task order and when selected for the task orders, the provisions listed here are binding.

**Project Manager – (Key Personnel)**

Leading cross-functional project teams to ensure the successful execution and delivery of projects on time, within scope, and within budget. This role involves planning, coordinating, and communicating with stakeholders at all levels while maintaining high standards of quality and performance. Define project scope, goals, and deliverables in collaboration with stakeholders. Develop detailed project plans, timelines, and budgets, ensuring alignment with organizational objectives. Identify project stakeholders and establish effective communication channels. Identify potential project risks and develop mitigation strategies to address them proactively. Monitor and report on risk status throughout the project lifecycle. Ensure that project deliverables meet established quality standards and stakeholder requirements. Maintain comprehensive project documentation, including project charters, status reports, and final deliverables.

**Roles and Responsibilities**

* + Work directly with Federal Program Manager (FPM), who establishes direction, priorities, and provides overall operational guidance.
  + Possess a working knowledge of the Agile Framework, which is based on Agile, Lean, Scaled Agile Framework (SAFe) principles. Has a working knowledge of project management concepts.
  + Provide direct support and advice to FPM and Federal team.
  + Manage and provide daily oversight of vendor staff.
  + Provide deliverables in an iteration while tracking and removing any impediments.
  + Confirm adequate resources for projects.
  + Serve as principal contractor interface with the Contract Officer’s Representative (COR) and FPM and other Federal staff.
  + Manage project scope, deliverables, and schedule.
  + Be responsible for project execution and must be able to create release and project plans including deliverables and the release deadline, planning and estimating the highest value deliverables for the next release, and ensuring that the team lives by the agile practices and rules of Scrum and its values (achieving specific milestones through accurate forecasting).
  + Manage work of all contractor and subcontract staff assigned to the Contract such that activities and deliverables are completed on time and to the customer’s satisfaction.
  + Directly oversee and participate in activities requiring senior technical and management skills, as appropriate.
  + Hold regular (weekly minimum) status meetings with Federal team members to provide and receive perception and input into ongoing support requirements.
  + Assist the FPM with tasks associated with formal meetings, (e.g., establishment of agenda, meeting minutes, tracking status of action items and deliverables, etc.).
  + Prepare and present progress reports for senior Federal management and stakeholders.
  + Confirm project documents are complete, current, delivered on schedule, and archived appropriately.
* Prepare and submit all required reports to Contract Officer (CO) and COR
* Apply project methodology (such as, scoping, planning, designing, building, deploying, and closing out project) using critical thinking and leadership skills.
* Provide input into security documents, assessments, and plans.
* Support a working environment conducive to effective collaboration
* Be responsible for training and building high-performing teams that support overlapping or separate data services, supporting project specific/OCIO stakeholders, and coordinating with other teams across the organization.
* Other duties as assigned.

**Experience/Qualifications**

* Previous development experience and federal experience can be a major plus.
* A minimum of ten-years of experience managing IT application development projects.
* A minimum of 3-years of experience managing teams of 4 or more people utilizing agile methodology (Scrum and Kanban).
* Certified Scrum Master.
* Experience with project management software (Jira, Confluence, Git).
* Experience leading large, cross-discipline projects.
* Experience prioritizing deliverables with sprint planning and managing sprint schedules.
* Experience managing a healthy backlog with changing priorities.
* Experience working with development team to produce accurate work estimates.

**Education and Certification(s)**  
Bachelor’s degree in business, or Project Management, or a directly related field with 5 years of current management experience, preferably in the federal sector. Active Agile certification.

**AI Architect, Senior (Key Personnel)**

Duties: Lead the design and architecture of AI solutions. Develop scalable AI models and algorithms to address business needs. Identify opportunities for applying AI technologies to improve business processes. Work closely with data scientists, engineers, and stakeholders to integrate AI solutions. Coordinate with cross-functional teams to ensure successful deployment of AI projects. Provide technical guidance and mentorship to junior architects and team members. Review and approve design and code. Stay updated with the latest AI trends and technologies. Evaluate and implement new tools and frameworks to enhance AI capabilities. Ensure AI solutions comply with relevant laws and ethical standards. Implement security best practices in AI systems. Maintain comprehensive documentation of AI architectures and processes. Provide training and support to end-users and staff on AI applications.

**Roles and Responsibilities**

* Collect and preprocess data for training models.
* Develop and train machine learning models using appropriate algorithms and techniques.
* Evaluate model performance using metrics such as accuracy, precision, recall, and F1 score.
* Tune hyperparameters and adjust model architecture to enhance performance.
* Deploy models to production environments, including cloud platforms and API endpoints.
* Continuously monitor model performance and adjust to maintain accuracy and reliability.
* Collaborate with cross-functional teams, including data scientists, data engineers, and software developers.
* Stay informed about the latest advancements in machine learning and NLP research, applying them to improve model performance.
* Work with Federal government customers in understanding agency missions and associated project objectives. This includes working with customers to gain an understanding of key pain points, project requirements, constraints, and potential RFP evaluation criteria.
* Proven experience working as an Enterprise Machine Learning Architect or in a similar technical leadership role. Must have successfully implemented large-scale ML solutions in an enterprise environment, aligning with organizational goals.
* Stay up to date with emerging technologies, industry trends, and best practices related to application development, cloud computing, data, cybersecurity, AI, and ML.
* Demonstrated expertise in identifying high-impact business use cases for machine learning across various departmental functions such as data analytics, security, HR, finance, and more. Experience in designing and implementing scalable, innovative ML solutions that meet the strategic objectives of the organization.
* Strong ability to assess and define the role of machine learning within the enterprise's broader goals. Must have an encompassing view of how ML can be applied across multiple domains to drive business value and efficiency.
* Comprehensive understanding of how ML integrates with different enterprise systems and departments, including data platforms, security frameworks, human resources, finance, and more. Capable of working with cross-functional teams to deliver solutions that span the entire enterprise.
* Proven ability to work with senior leadership and stakeholders to communicate the value of ML initiatives. Experience in driving organizational change through ML and AI-driven projects, ensuring alignment with business priorities.
* Strong commitment to implementing Responsible AI principles, including fairness, accountability, transparency, and ethics in machine learning applications. Must have experience designing AI solutions that are compliant with regulatory standards and enterprise governance, while ensuring ethical use and minimization of bias in AI models.
* Experience overseeing the entire ML lifecycle, from data preparation and model development to deployment and monitoring. Should have worked closely with Data Science, ML Ops, and DevOps teams to ensure operationalization, governance, and continuous monitoring of ML models.
* Familiarity with productivity improvement tools such as Amazon Q for efficient data querying or Copilot for intelligent code suggestions, upgrades and automated documentation, enhancing coding efficiency and streamlining the development process for machine learning workflows.

**Experience/Qualifications**

* Strong understanding of both supervised and unsupervised learning algorithms, as well as deep learning models.
* Proficiency in Natural Language Processing (NLP), text mining, feature engineering, and data preprocessing techniques.
* Proficient in programming languages such as Python, R, or Java.
* Experience with machine learning frameworks such as TensorFlow, Keras, or PyTorch.
* Experience with cloud platforms like AWS, Azure, or Google Cloud Platform.
* Strong analytical and problem-solving skills.
* Excellent communication abilities for effective collaboration and reporting.
* Experience in Authority to Operate (ATO) preparation.
* Minimum 8 years of experience in solution architecture in AI/ML systems, including data pipelines, model training, and data analytics.
* Expertise in designing scalable, fault-tolerant, and high-performance machine learning architectures in cloud environments(preferred) such as AWS, Azure, or Google Cloud. Must have hands-on experience with managed ML services such as AWS SageMaker, Azure Machine Learning, or Google AI Platform (Machine Learning as a Service – MLaaS).
* Experience with Integration Platform as a Service (iPaaS) solutions for integrating machine learning models into enterprise applications
* Proven experience with ML model quality control, including techniques for ensuring robustness, fairness, and accuracy. Expertise in setting up continuous model monitoring, drift detection, and alerting systems.
* API Integration & External Interconnectivity: Strong experience in designing and deploying machine learning models that integrate with external enterprise systems via RESTful APIs or iPaaS platforms. Experience in securely connecting to external data sources and third-party services to enhance ML models and applications.
* Generative AI (GenAI) & Large Language Models (LLM): Hands-on experience with Generative AI solutions and LLMs like Amazon Bedrock, OpenAI GPT, or similar. Ability to leverage these technologies to design, deploy, and fine-tune models for enterprise use cases, including chatbots, automated content generation, and knowledge management.
* Agents & Agentic Code Interpreters: Expertise in building and deploying AI Agents capable of autonomously conducting tasks, running code, and making decisions based on context. Experience with Agentic Code Interpreters, such as those available through Amazon Bedrock or OpenAI Code Interpreter, to enable complex problem-solving and dynamic task execution.
* Retrieval-Augmented Generation (RAG): Familiarity with RAG techniques to enhance LLMs by retrieving relevant knowledge from external sources (such as document databases or APIs) in real-time, improving the accuracy and relevance of AI outputs.
* ML Frameworks & Libraries: Proficiency in popular machine learning frameworks and libraries.
* Data Engineering & Pipeline Orchestration: Experience with building and managing data pipelines using Apache Airflow, Kubernetes, AWS Glue, or Azure Data Factory or similar. Strong knowledge of ETL (Extract, Transform, Load) processes and tools like Apache Spark, Databricks, and Snowflake.
* Model Deployment & MLOps: Extensive knowledge of deploying machine learning models at scale using MLOps best practices. Familiarity with CI/CD pipelines for ML models. Experience with managing model versioning, retraining, and continuous monitoring in production.
* Expertise in leveraging MLaaS platforms such as Google AI Hub, AWS SageMaker Studio, and Azure AI for rapid development, training, and deployment of machine learning models. Knowledge of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) for efficient infrastructure management and application hosting.
* Strong understanding of data governance practices, security, and compliance within an enterprise environment. Experience with implementing data privacy and regulatory compliance in machine learning workflows. Experience with IAM (Identity and Access Management) policies and role-based access control for data and model security.
* In-depth knowledge of Responsible AI principles, including model explainability, fairness, accountability, and bias detection. Must have experience implementing transparent and interpretable AI models with ethical considerations in mind.
* Advanced knowledge of database management systems, including SQL (e.g., PostgreSQL, MySQL) and NoSQL (e.g., MongoDB, Cassandra, DynamoDB). Experience with data lakes and data warehouses, such as AWS Redshift, Google BigQuery, or Snowflake.
* Proficiency in cloud infrastructure management and automation using tools like AWS CloudFormation, Azure Resource Manager, and Google Cloud Deployment Manager. Knowledge of infrastructure-as-code (IaC) and cloud orchestration tools such as Terraform and Ansible.
* Ability to work with Data Scientists to translate business requirements into ML models. Familiarity with Python, R, and Jupyter Notebooks for collaborative development. Knowledge of ML Workflow Automation through MLaaS platforms to streamline the experimentation and deployment process.

**Education and Certification(s)**

* Bachelor’s degree in computer science, Information Management (IM), Information Technology, Engineering, Data Science, or equivalent with 8 years of technical experience, or 6 years’ experience in IT Solutions as a hands-on lead and architect (preferred)
* AWS Certified Solutions Architect (Highly Recommended)
* Google Cloud Professional Cloud Architect (Optional)
* Microsoft Certified: Azure Solutions Architect Expert (Highly Recommended)

**Data Scientist (Key Personnel)**

Duties: Captures, processes, manages, and analyzes large data sets using advanced techniques, including natural language processing, cluster analysis, image analysis, pattern recognition, predictive modeling, and visualization. Hands-on development and engineering of large-scale data science solutions, preferably in production environments. Ensures that Data Pipelines, Machine Learning Pipelines, and Monitoring activities are established for Continuous Integration, Continuous Development, and Continuous Testing. Serve as the primary resource for machine learning lifecycle issues and provide expert insights for identifying data patterns, including both pattern and anomaly detection. Proficiency in statistical software like R, Python, SAS, or SPSS, and experience with at least one cloud platform, such as AWS, Azure, or GCP, is essential. Visualize and report findings to stakeholders using various visual formats and adapt presentations to audiences with different technical levels. Establish and maintain data collection and storage systems, programs, and procedures to build analytic systems, ensuring accurate and efficient data management. Additional duties are performed as assigned.

**Roles and Responsibilities:**

* Analyze large datasets to identify trends and insights.
* Develop predictive models and validate their performance.
* Work closely with stakeholders to understand business needs and define project requirements.
* Collaborate with engineers to implement models into production systems.
* Stay current with industry trends and apply best practices in data science.
* Conduct exploratory data analysis (EDA) to understand data patterns, trends, and anomalies.
* Utilize statistical methods to derive insights from data and inform business decisions.
* Clean, preprocess, and transform raw data into usable formats, ensuring data quality and integrity.
* Handle missing data, outliers, and perform feature engineering to enhance model performance.
* Design, implement, and evaluate predictive and prescriptive models using machine learning algorithms.
* Experiment with various algorithms (e.g., regression, classification, clustering) to identify the best fit for specific problems.
* Work closely with business stakeholders, product managers, and engineers to understand business objectives and translate them into data-driven solutions.
* Communicate findings and insights to non-technical audiences through visualizations and presentations.
* Assist in deploying machine learning models into production environments, ensuring scalability and reliability.
* Monitor model performance post-deployment and iterate based on feedback and changing data patterns.
* Stay updated with the latest advancements in data science, machine learning, and artificial intelligence to implement best practices.
* Conduct research on new methodologies and technologies that can enhance data science capabilities.
* Document data science processes, models, and methodologies for reproducibility and knowledge sharing.
* Create comprehensive reports summarizing analysis results, methodologies, and recommendations for stakeholders.
* Implement ethical considerations in data science practices, ensuring fairness, transparency, and accountability in model predictions.
* Evaluate models for bias and fairness, proposing adjustments where necessary to adhere to responsible AI principles.

**Experience Required:**

* Proficiency in machine learning algorithms and statistical modeling techniques.
* Experience with data analysis, feature selection, and dimensionality reduction.
* Proficient in programming languages such as Python or R.
* Familiarity with machine learning libraries and tools like Scikit-learn, Pandas, and NumPy.
* Experience in data visualization tools (e.g., Tableau, Matplotlib).
* Strong communication skills to translate complex findings into actionable insights.
* Understanding of business processes and ability to align data projects with organizational goals.
* Minimum 4+ years of experience as Data Scientist in exploratory data analysis, modeling on structured and unstructured data sets
* Proficient in programming languages such as Python or R for data manipulation, analysis, and modeling. Familiarity with SQL for querying databases and retrieving data efficiently.
* Experience with libraries such as Pandas, NumPy, and Dask for data manipulation and analysis. Knowledge of Matplotlib, Seaborn, or Plotly for data visualization.
* Expertise in machine learning libraries and frameworks like Scikit-learn, TensorFlow, Keras, and PyTorch. Familiarity with ensemble methods, deep learning architectures, and model evaluation techniques.
* Strong foundation in statistical concepts, hypothesis testing, and experimental design. Ability to perform advanced statistical analyses using tools such as Statsmodels or SciPy.
* Experience with big data technologies such as Apache Spark, Hadoop, or Kafka for processing and analyzing large datasets. Familiarity with distributed computing frameworks for scalable data processing.
* Ability to create compelling visualizations using Matplotlib and Seaborn. Model Deployment and MLOps:
* Knowledge of machine learning operations (MLOps) practices for deploying and maintaining ML models in production.
* Experience working with cloud platforms such as AWS, Azure, or Google Cloud for data storage, processing, and machine learning services.
* Experience implementing secure data practices and ensuring compliance with data policies.
* Strong verbal and written communication skills to convey complex technical concepts to non-technical stakeholders.
* Ability to work collaboratively in cross-functional teams, promoting data-driven decision-making.
* Experience in evaluating model performance using metrics such as confusion matrix, accuracy, precision, recall, F1 score, and R² (R-squared). Ability to interpret these metrics and effectively communicate their implications to stakeholders for informed decision-making and model enhancement.

**Education and Certification(s):**

* Bachelor’s degree in computer science, Information Management (IM), Information Technology, Engineering, Data Science, or equivalent with 3 years of technical experience

**Education and Certification(s)**

* Bachelor’s degree in computer science, Information Technology, Engineering, Data Science, or equivalent with 3 years of technical experience, or 6 years’ experience as a Data Scientist
* AWS Certified Solutions Architect (Highly Recommended)
* Google Cloud Professional Cloud Architect (Optional)
* Microsoft Certified: Azure Solutions Architect Expert (Highly Recommended)

**ML Engineer with MLOps Experience (Key Personnel)**

Duties: Responsible for developing models to automate processes and training models. This includes studying and transforming data science prototypes, selecting suitable data sets, and conducting data collection and modeling. Perform statistical analysis to enhance model performance. Engaged in end-to-end development, exploring innovative applications and techniques in natural language processing, applied machine learning, and explainable, privacy-aware AI/ML.

**Roles and Responsibilities:**

* Deploy machine learning models to production environments with robust monitoring and logging.
* Automate workflows for data collection, model training, and deployment.
* Implement CI/CD pipelines for machine learning projects.
* Monitor models in production and optimize performance over time.
* Work with data scientists to transition models from development to production.
* Document processes and provide knowledge transfer to teams.
* Evaluate and apply new tools and technologies to enhance MLOps practices.
* Develop and implement deployment pipelines for machine learning models in production environments. Monitor and manage the lifecycle of machine learning models, ensuring they are up-to-date and performing optimally.
* Work closely with data scientists to understand model requirements and integrate their solutions into production systems. Assist in the transition of models from experimentation to production, ensuring reproducibility and reliability.
* Design and automate infrastructure for model training, deployment, and monitoring. Implement CI/CD (Continuous Integration/Continuous Deployment) practices for machine learning workflows.
* Set up monitoring systems to track model performance, data drift, and anomalies post-deployment. Implement strategies for retraining and updating models based on new data and changing requirements.
* Develop and maintain ML data pipelines for collecting, processing, and feeding data into machine learning models. Ensure data quality and integrity throughout the pipeline, addressing issues proactively.
* Implement security measures to protect sensitive data and ensure compliance with regulations and best practices. Collaborate with IT and security teams to establish protocols for secure model deployment.
* Document processes, workflows, and best practices for model deployment and maintenance. Share knowledge and best practices with team members to promote collaboration and continuous improvement.
* Set up monitoring systems to track model performance, data drift, and anomalies post-deployment. Implement strategies for retraining and updating models based on new data and changing requirements.

**Experience Required:**

* Experience in developing and deploying machine learning models at scale.
* Proficiency with machine learning frameworks such as TensorFlow, PyTorch, or similar.
* Experience implementing MLOps principles, including version control and continuous integration/continuous deployment (CI/CD).
* Familiarity with infrastructure automation tools (e.g., Docker, Kubernetes).
* Experience with cloud services (e.g., AWS SageMaker, Azure ML) and implementing APIs for model deployment.
* Minimum of 2+ years of experience in MLOPS
* Proficient in programming languages such as Python or R.
* Familiarity with machine learning libraries and frameworks like Scikit-learn, TensorFlow, and PyTorch.
* Experience with cloud platforms such as AWS, Azure, or Google Cloud, particularly their machine learning services and infrastructure offerings.
* Knowledge of services like AWS SageMaker, Azure ML, or Google AI Platform for managing ML workloads.
* Familiarity in containerization technologies like Docker and orchestration tools such as Kubernetes for deploying scalable ML solutions.
* Experience implementing CI/CD pipelines using tools like Jenkins, GitLab CI for automating machine learning workflows.
* Knowledge of data engineering concepts and tools such as Apache Airflow, Apache Kafka, or Apache Spark for building and managing data pipelines.
* Experience with model versioning and management
* Familiarity with AWS SageMaker Model Monitor for tracking model performance and detecting data drift, along with AWS CloudWatch for logging and monitoring system health and performance metrics.

**Education and Certification(s)**

* Bachelor’s degree in computer science, Information Technology, Engineering, Data Science, Artificial Intelligence or equivalent with 3 years of technical experience, or 6 years’ experience as a Data Scientist
* AWS Certified Solutions Architect (Highly Recommended)
* Microsoft Certified: Azure Solutions Architect Expert (Highly Recommended)
* Google Cloud Professional Cloud Architect (Optional)

### 1.7.2 Organizational Conflict of Interest:

Contractor and subcontractor personnel performing work under this contract action may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI), as defined in FAR Subpart 9.5. The contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The contractor’s mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the contractor from participation in subsequent contracted requirements which may be affected by the OCI.

### 1.7.3 Phase In/Phase Out Period

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the contractor shall have personnel on board during the phase in/phase out periods. During the phase in period, the contractor shall become familiar with performance requirements in order to commence full performance of services on the contract action start date.

# Part 2

## Definition & Acronyms

**BAS. Business Application Services,** a unit of DOL OASAM OCIO which manages all business-focused projects throughout the development lifecycle.

**Best Effort**: That effort expended by the contractor to perform within the awarded ceiling price all work specified in this acquisition and all other obligations under this acquisition. This effort includes providing required qualified personnel, properly supervised, and following industry accepted methodologies and other practices. The effort is further characterized by operating at all times with the government’s best interest in mind, using efficient and effective methods, and demonstrating sound cost control. The effort must be identical to the effort that would be expended if this were a firm-fixed price acquisition, and the contractor’s profits were dependent upon reducing costs while meeting the government’s requirements in terms and quality and schedule. Failure to provide this required effort may result in the withholding of payment for hours expended that do not qualify as best effort or a reduction in the rate per hour to reflect decreased value of services received.

**Contracting Officer’s Representative.** A representative from the requiring activity assigned by the Contracting Officer to perform surveillance and to act as liaison to the contractor

**Defective Service**. A service output that does not meet the standard of performance associated with it in the Performance Work Statement.

**MVP.** Minimum Viable Product

**OASAM.** Office of the Assistant Secretary for Administration & Management, an agency within DOL which provides the infrastructure and support that enables DOL to perform its mission.

**OCIO**. Office of Chief Information Officer. An office within DOL OASAM dedicated to providing IT solutions and leadership to advance DOL’s mission.

**Quality Assurance (QA)**. Those actions taken by the government to assure services meet the requirements of the Performance Work Statement.

**Quality Assurance Surveillance Plan (QASP)**. An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

**Quality Control (QC)**. Those actions taken by a contractor to control the performance of services so that they meet the requirements of the PWS.

# Part 3

## Government Furnished Property, Equipment, And Services

## General:

The government will provide the facilities, equipment, materials, and/or services listed.

below.

## Equipment:

* DOL Laptops and associated helpdesk support
* DOL Personal Identity Verification (PIV) cards
* Software/services deemed necessary for the performance of this work which may include Jira for change management and Git for code repository.

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material or Contractor-Acquired-Government Owned Property (CAP). The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each monthly report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor’s inventory listing must be available for Government review within one business day of COR request.

Access that is granted and not used may expire. The contractor shall take steps to ensure its staffing plan and staff are appropriately using the access granted to them and access does not expire. Mandatory and annual trainings must be completed to obtain and maintain access.

## Facilities:

Remote. The contractor will furnish necessary equipment to perform the effort(s) outlined in this PWS remotely, at a location other than a government-owned or contractor-owned facility. If deemed necessary, the government may issue, at its discretion, supplemental equipment (e.g., computing equipment).

# Part 4

## Contractor Furnish Items and Services

## 4.1 General:

Except for those items specifically stated to be government furnished in Part 3, the contractor shall furnish all other items required to perform the services in this PWS.

## 4.2 Clearance:

The Contractor shall possess or be eligible to receive and maintain an unclassified clearance. The Contractor’s employees, performing work in support of this contract shall have been granted an unclassified security clearance.

# Part 5

## Specific Tasks

The contractor shall provide services for:

* Services
* Transition-In
* Program and Project Management
* System/Application Development, Operations, and Maintenance
* Training
* Transition-Out

## Services

The contractor shall perform the **development** tasks as listed in Technical Exhibit 3.

### Task Area 1: Artificial Intelligence

Contractor must provide AI Implementation Services which includes Use case discovery, ideation, proof of concept/proof of value, development, deployment, production, O&M, and monitoring. The AI implementation services, which include products and solutions, will be designed to seamlessly integrate and develop government and industry practices across the DOL IT portfolio of applications.

The AI activities are inclusive of, but d not limited to designing, delivering, and supporting custom models, and using GEN AI technologies to develop enterprise services, capabilities, applications, and utilities using CSPs, COTS  products, and Open Source and by integrating AI custom models into existing applications and services, extending the solution to enhance Generative AI use cases, and leveraging established AI technologies and principles such as data preprocessing, feature engineering, model training, and model evaluations. The desired outcome is a future-proof framework/capability/process that is efficient, extensible, future-proofed, and tailored to the needs of the DOL.

The Contractor must create a model factory and a model marketplace to facilitate the deployment and management of AI models as required.

The AI solution delivery must use enterprise agile in compliance with all DOL OCIO IT/AI/Data/Security/ Agile requirements and guidelines which are based on public sector AI/IT requirements such as White House Executive Order, OMB, NIST Risk Management Framework and are also based on industry best practices, standards, and frameworks such as Agile, CRISP-DM (Cross-Industry Standard Process for Data Mining), and TDSP (Team Data Science Process). The Contractor will collaborate with stakeholders to identify business needs, gather requirements, and prioritize features aligned with strategic goals. The AI solution will be scalable enterprise wide, extensible, and adaptable to accommodate evolving business needs and emerging technologies.

Additionally, the solution and products must comply with the NIST (National Institute of Standards and Technology) and Responsible AI standards set by federal government agencies. The implementation will include features such as logging, monitoring, auditing, securing (static and dynamic scanning), artifact management, and thorough testing to ensure the readiness of the solution for enterprise deployment. These measures will help maintain compliance, security, and accountability throughout the AI implementation process.

### Task Area 2: Advanced Engineering

* Develop and review policies and processes in supporting the DOL enterprise architecture program and any projects within IT system Engineering and Integration Support services.
* Design, develop and/or peer-review architectures, and conduct implementations for engineering projects at DOL.
* Support platform infrastructure associated with AI/ML and Robotic Process Automation initiatives.
* Intake and assessment of agency Demands/use cases
* Develop and review policies and processes supporting TIE
* Supports establishing DOL-wide Electronic Records Management (ERM) standards and governance.
* Provide engineering support to the ERM team

### Task Area 3: Electronics Records Management

* Continued technological and project management support of DOL Electronic Records Management System (eRMS) and Metadata/Taxonomy for electronic records management
* Meetings and project management support for a litigation hold system
* Future Enterprise Digitization/Scanning of paper/analog records
* Continue to align records management strategic goals with OCIO to meet M-23-07
* IT Modernization and Information Governance goals as aligned with records management strategic plan
* Records Management for All and Controlled Unclassified Information (CUI) training in Learning Link
* Support in intranet site redesign for Records Management pages
* Manage DOL contract for the design, development and implementation of the Electronic Records Management Platform
* DOL baseline taxonomy

### Task Area 4: Emerging Technology

Contractor services needed for Emerging Technology task area are inclusive of, but not limited to Quantum Computing including activities related to post quantum crypto readiness and quantum algorithms, support for innovative technologies such as Augmented Reality & Generative AI, ability to evaluate and bring in new technologies and services to the DOL ecosystem as required by DOL**.**

### Task Area 5: Enterprise Architecture

The Contractor shall provide architecture and engineering service support for the following:

Enterprise Architecture: Expertise to abide by and help develop DOL’s Strategic Roadmap in support of ensuring OCIO technology strategy serves their business strategy by:

* Maintaining Governance awareness of larger Federal initiatives and policy
* Developing, managing and maintaining an OCIO Service portfolio
* Assessing the current as-is state and recommending Future state for each OCIO service as well as incremental plan to achieve this state.
* Work with other DOL divisions to develop the enterprise-wide standards and reference architectures to guide IT delivery.
* Discovery and Inventory: This task will consist of conducting an automated inventory of the as-is state of DOL’s environment.
* Facilitate the creation of a Business Capability Model
* Maintain IT Data Model roadmap.
* Develop New software intake process
* Support OMB and internal Data calls
* Manage the Reference Architecture
* Support IT Modernization
* Mange the IT Modernization Score card
* Facilitate Cross Functional expertise in the ITARB evaluations.
* Working with AE and TIE SORT team provide solutions Design.

**Task Area 6: Mobile Application Development**

The contractor shall provide services for Mobile App Development. The contractor shall be able to adapt and provide the necessary resources (project management, business analysis, design, and development) to maintain minimum throughput and work in progress (WIP) service levels agreed to between OCIO and its customers.

The maintenance and development support includes the following major areas:

* Project Management
* Mobile Application Design, Development, Testing, and Support

**Task Area 7: Security Solutions**

Contractor services needed for Security Solutions task area are inclusive of, but not limited to:

* Establishing measurable security risk management frameworks compliant with federal standards such as NIST RMF, NIST AI RMF, and all Office of the Chief AI Office (OCAIO), Chief Technology Officer (CTO), DOL requirements.
* Implementing and managing enterprise security tools, solutions, processes, and monitoring.
* Ensuring security for all AI systems using measurable and repeatable processes.
* All Post Quantum Crypto (PQC) readiness activities including developing approaches and supporting DOL’s platforms, applications, tools, data, information, and services for PQC safety.

## Transition-In

Transition-In shall commence upon Task Order award, for a total of 45 days, with 15 of these calendar days dedicated to the onboarding process. During this time, the Contractor shall go through an onboarding process which includes background investigations to obtain DOL badges, DOL laptops, access to DOL’s systems and network, and applicable government furnished information (GFI).

The Contractor shall perform the following Transition-In tasks:

* Onboard contractor employees, i.e., complete background screening, obtain DOL badges, laptops, network, and systems access.
* Provide a list of anticipated required software necessary to support this task order to the COR and Fed PM.
* Ensure contractor employees understand their roles and responsibilities along with the requirements of this Task Order, i.e., deliverables/timelines, Agile framework, deployment environment, and required templates.
* Interview the COR, PM, and/or business stakeholders to fully understand and assess the use cases, as well as applicable documentation.
* Report Transition-In activities, risks, and issues during the weekly status meetings
* Ensure an understanding of the existing systems documentation, source code, systems architectures, and planned releases.
* Review the backlog of requirements.
* Attend Technical Exchange Meetings (TEMs) with the outgoing Contractor to gain knowledge of the systems and activities, including sustainment.
* Ensure contractor employees understand and are proficient with all DOL agile, development, security, 508, performance, testing, communication, and delivery standards.
* Provide a comprehensive plan to product owner, FedPM, and Federal technical stakeholders that validates assumptions and includes artifacts such as agile release train, MVP, test plan, JIRA (Confluence, Portfolio) backlogs, architecture, data dictionary, etc.

## 5.3 Program and Project Management

The Contractor shall provide project management to establish control, management, monitoring and notification mechanisms, ensuring that all requirements within the PWS stay on track and milestones and performance measures are met. The Contractor shall plan, organize, control, and staff the technical, administrative, financial, contractual, and personnel actions as required to perform this task order.

The Contractor shall maintain quality control throughout the duration of the contract through repeatable, managed processes that are equivalent to DOL Quality Assurance Surveillance Plan (QASP)

* Work with Federal system owners, product owners, and subject matter experts to validate functional requirements provided by product owner and refine or perform further requirements gathering and analysis as needed.
* Update requirements in JIRA and/or system requirements documentation as needed.
* The contractor shall share and post in JIRA user story supporting documentation, test case documentation, test scripts, and any specific information relating to an epic, user story, task, or sub task.
* The Contractor shall share and post at a DOL Share Point location all system documentation, which includes requirements specification beyond the JIRA documentation, design documentation, network diagrams, deliverables, and other overarching documentation.
* The Contractor shall update DOL’s suggested PPM tool for the project with all artifacts required by OCIO PMO and be responsible to move it through the stage gates by completing all requirements identified in each checklist.
* The Contractor shall maintain and update detailed System Design analysis, Architecture Overview, and Business workflows.
* Maintain a risk register which identifies risks and mitigation plans, and provides for special emphasis on cost controls, time management, continuous improvement, and ongoing contract monitoring.
* Work collaboratively with DOL stakeholders to maintain a target architecture.
* Maintain a project review process where, on a scheduled basis, the project manager provides status reports demonstrating cost performance, schedule performance, resource management, achievements, and projections.
* Provide invoice detail reports including monthly burn-rate projections which form the basis for actual costs reported and tracked in the integrated baseline plan and for earned value management performance monitoring.
* Provide hour usage breakdown by individual name to include hours worked and Labor Category of each employee.
* Provide a contract personnel report which includes all personnel working on the contract and those who have departed the contract. Information shall include at a minimum, name, work telephone number, work email address, home contact info, GFE make/model/serial number, virtual telephone number, duty description, certifications/qualifications as required by role, work schedule, extended time off.
* Track the allocation and consumption of funds on the contract by each task order and provide advanced warning of funding shortfalls using financial burn rate charts.
* Identify and communicate to the Government all necessary software, hardware, licenses, or equipment required in support of the performance of this contract.
* Work collaboratively with DOL stakeholders to create and maintain documentation in support of Enterprise Architecture and Capital Planning & Investment Control.
* Provide DOL stakeholders with formal briefings as requested.
* Provide a weekly status briefing for the Federal PM.
* Include Fed PM on any communications with Program Office, OCIO areas, or other agencies.
* Provide bi-weekly sprint planning, backlog grooming and refinement, daily SCRUM, sprint retrospective, and other meetings as directed and approved by the Fed PM.

### 5.3.1 Task Order Management Plan

The Contractor shall develop a Task Order Management Plan (TOMP) for Government approval that will include a resource and cost loaded schedule which documents dates for all key activities, deliverable due dates, and associated staffing levels of effort for each activity. When identifying key activities, the Contractor shall consider how they will work with the existing system architecture and identify an appropriately tailored workflow. Following Government approval of the plan, it shall be applied by the Contractor to manage the task. The Task Order Management Plan shall include, but not be limited to, the following:

* A resource-loaded schedule which documents dates for all key activities, deliverable due dates, and associated staffing levels of effort and costs for each activity
* Identification of milestones or activities where Government information, activity, equipment, material, facilities, etc. is required and timeline dependencies for subsequent Contractor activities
* A detailed staffing plan with key personnel approved by the Government
* Approach and timeline to achieve Minimum Viable Product (MVP)

### 5.3.2 Integrated Project Team (IPT)

The Contractor shall participate in IPTs if identified by the FPM. As a result, the Contractor shall participate in the IPT which will include federal and other contractors. The contractor is expected to work collaboratively and proactively with other contractors as part of these IPTs to create a “one team” environment. The team shall:

* Participate in integrated SCRUM teams consisting of federal staff, contract staff from multiple vendors, and other cross-DOL team members as required
* Participate in the rating of integrated teams (contractors and Federal Department) during Retrospectives at the end of designated Sprints
* Participate in survey assessments that will seek input from partnering Contractors through the use of a federal survey. The survey will be provided to each contractor to rate each of the participants. Utilize a rating scale of 1 through 10 – where 10 is the higher value – along with a section that provides an area to provide comment. The surveys will be averaged across all participants to determine an average rating. Comments received will be shared with all participants
* Produce deliverables (business process diagrams, system design documents, data architecture designs) that will be used by SCRUM teams to develop solutions

### 5.3.3 Monthly Progress Report

The Contractor shall prepare and deliver a Monthly Progress Report (MPR). The MPR shall outline deliverables submitted, problems encountered, and schedule deviations. The MPR shall measure the Contractor’s price and schedule performance using measures as mutually agreed upon by the Government and the Contractor. The report shall include the current price and level of effort.

## 5.4 System/Application Development, Operations, and Maintenance

The Contractor will focus on user’s needs being fully represented in product design and development, use a platform to rapidly develop applications, and allow for the design and implementation of system enhancements that further improve the user experience. The Contractor will bring the necessary tools for all aspects of development, maintenance, testing, measuring, and reporting to the task; the Government will be responsible for the ownership of the core component (e.g., the platform, databases, and content management systems).

The Contractor will provide the skilled resources necessary to manage the design, application development, testing, and deployment. System/application development, operations, and maintenance requirements include but are not limited to:

* Monitor system performance and report statistics
* Manage and operate relevant system components not covered under third party control (e.g., Government and Commercial FedRAMP Services)
* Provide technical support and written assessments relating to the integration of new services or software products into the system environment
* Manage and provide functional requirements gathering, change control processes, feasibility studies, and cost benefit analyses.
* Develop use-case scenarios and other information necessary to provide functionality satisfying Government needs
* Develop applications and code which meets requirements and applicable DOL and Government standards
* Conduct and manage testing activities for software releases
* Provide documentation for all development code and create support manuals
* Ensure all system code is maintained in a DOL OCIO code repository
* Support other Program tasks in creating reports, documentation, or deliverables
* Develop and maintain in DOL OCIO Jira/Confluence requirements, user story supporting documentation, test case documentation, test scripts, and any specific information relating to an epic, user story, task, or sub task
* Develop and maintain in a DOL repository detailed System Design documentation including architecture and business workflows
* Develop and maintain in a DOL repository a Configuration Management plan that includes the workflow of change requests and defects, change control board roles and responsibilities, and procedures for managing code baselines and documentation including a database to track change requests and defect reports
* Support identification and procurement of all required hardware, software and other required resources to support the system
* Coordinate all operations, maintenance and enhancement activities with the hosting provider, independent Contractors, and other relevant stakeholders

### 5.4.1 Operations Support Services

The Operations Support Services is to provide operational production support activities that focus on the routine support required to maintain the availability of the system. Example operational activities include corrective actions, resolving end user reported bugs, production system outages, updating documentation, and critical security findings that require immediate action.

The Contractor shall provide the full range of operational support services in accordance with DOL agile processes utilizing the DOL agile products such as Jira Software to plan, execute, and report on progress.

The anticipated level of support to meet this objective is one operations-based agile team to maintain operational status of the system under a fixed price CLIN.

### 5.4.2 Maintenance Support Services

The Maintenance Support Services is to provide maintenance activities that focus on preventative support to maintain the reliability and security of the system while reducing technical debt. Example maintenance activities include server upgrades, operating system upgrades, middleware upgrades, database upgrades, replacing end-of-life components, software refactoring and optimization, and changing to use a new framework. Maintenance activities can also be the result of cyber security findings (Plan of Action and Milestones – POA&Ms) that are prioritized and scheduled for resolution.

The Contractor shall provide the full range of maintenance support services in accordance with DOL Agile processes utilizing the DOL agile products such as Jira Software to plan, execute, and report on progress.

The anticipated level of support to meet this objective is one maintenance-based agile team to maintain the system under a labor hours CLIN.

### 5.4.3 Development and Enhancements

Development is to implement a new project while Enhancements add new features to an existing project. Example development and enhancements activities may include creating new user types or forms, adding print functionality, changing from one factor authentication to multi-factor, etc. As a rule of thumb if it’s worth bragging about to customers/end users, then it’s development/enhancement, otherwise it’s considered maintenance.

The Contractor shall architect and create DOL Agile artifacts for any changes to the system. The Contractor shall provide the full range of maintenance support services in accordance with DOL Agile processes utilizing the DOL agile products such as Jira Software’s to plan, execute, and report on progress.

The anticipated level of support to meet this objective is one agile team to develop/enhance the system under a labor hours CLIN.

### 5.4.5 DevSecOps

The Contractor’s DevSecOps practices will automate testing and code/deployment promotion. The Contractor’s code pipeline will be based on containers and version control.

The contractor shall conduct and execute Sprint cycles which shall include requirements definition and prioritization, design specification, and a development and operational testing cycle. The contractor shall bundle the two-week sprint cycles into monthly production releases containing 2 sprints, unless otherwise approved in writing by the FPM.

The Contractor shall ensure that Cybersecurity is fully integrated into all phases of the software development process, including initial design, development, testing, and is part of the approval process. The Contractor shall ensure the proper Contractor support staff is available to participate in security test & evaluation and security authorization processes. This includes, but is not limited to:

* Attending and supporting security meetings with the Government
* Supporting/conducting the vulnerability mitigation process
* Supporting the Assessment Team during system security testing
* Defining the security authorization boundary
* Correcting or adequately mitigating security vulnerabilities
* Documenting configuration baselines

The Contractor’s Detailed System Design documentation shall:

* Describe its DevSecOps processes and environments.
* Address the Ports, Protocols, and Services (PPS) proposed to be used to transport data and communicate between systems.
* Identify all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface
* Identify user roles required for access control and the access privileges assigned to each role
* Address unique security requirements (e.g., encryption of key data elements at rest)
* Identify categories of sensitive information processed or stored by the application, and their specific protection plans (e.g., Privacy Act, HIPAA)
* Contain or point to a current and comprehensive baseline inventory of all software and services supporting the system (to include manufacturer, type, and version and installation manuals and procedures)
* Illustrate how all user interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems).

### 5.4.6 Test Plan & Execution

In addition to testing and in preparation for the Production Releases, the Contractor  
shall coordinate and perform the following test activities:

* + - Unit Testing
    - System Integration Testing
    - Performance/Load Testing
    - 508 Compliance Testing (DHS Trusted Tester Certification preferred)
    - Regression Testing
    - User Acceptance Testing (UAT) – Facilitate and Assist
    - Develop test scenarios/cases for use during UAT
    - Provide for and support Zephyr testing within the Jira Instance
    - Web Inspect Testing (min 90 day per version frequency)

The Contractor shall modify and regression test code to resolve errors found to ensure the system is ready for production deployment. All changes shall be documented in the DOL OCIO’s change control/configuration management tools. Escaped defects and other CMMI/ISO standards metrics will be tracked in the PM workbook.

The Contractor shall document the test results and then upload the results to Jira as an attachment to the appropriate story, or in the case of a larger scope, to Confluence in the appropriate folder.

**Note**: Automated testing processes, including Zephyr, shall be used whenever possible.

### 5.4.7 Release Management

The Contractor shall provide Release Management support for the planning, preparation, scheduling, delivery, review, and testing of all system software releases and their supporting documentation. The Contractor’s approach shall reflect DOL’s release management process. The Contractor shall plan for system releases as directed and approved by the Federal Project Manager. The Contractor shall coordinate with appropriate development, testing, and support Contractors and advise the Federal Project Manager frequently on the status of planned releases. Software shall be submitted for release approval by the Contractor with:

* No in-sprint bugs
* Unit test report(s) (e.g., Data validation)
* Code review report(s)
* Section 508 test report(s)
* Mobile/tablet test report(s)
* Performance test report(s)
* Security test report(s)
* Code checked into Git (including deployment scripts)
* Updated release notes
* Updated labor expenditures
* Project-specific requirements and tasks completed
* Updated data dictionary/model where applicable
* Updated user guide(s) where applicable
* Updated system design/administration documentation where applicable
* Updated functional requirement documentation where applicable.

DOL OCIO maintains a shared development and version control environment for all application development. This requires all code to be maintained in a centralized Git repository, and a “check out / check in” process is required for authorized programmers to use in conducting assigned development tasks. The Contractor agrees to conform to DOL's policies and procedures governing the use of the shared development space.

The contractor shall Submit Incident Tickets and Change Requests in Service Now for all code changes and code promotions.

## 5.5 Training

The contractor may be asked to aid in the development of training. The Contractor shall train various parties, including but not limited to end users, internal and external customers, internal IT Service Desk staff, Operations staff, etc. The Contractor shall document and/or video each session of “train the trainer” and must be Section 508 compliant. The Contractor shall provide user guides for each deployed software application:

* Develop and maintain end-user documentation (user manuals, user guides, systems administration procedures, and training documents) one week prior to a major application release date.
* Supporting materials such as release notes, user manuals, and training manuals shall be in final form and shall also been verified by the Product Owner for quality assurance or other appropriate reviewers 1 week prior to a major application release date.

## 5.6 Transition-Out

The Transition-Out is to allow the incoming contractor to staff up to the appropriate support levels and participate in knowledge sharing with the outgoing contractor so that incoming staff can be prepared to fully support the system. During this time, the outgoing Contractor shall provide support services to the orderly transition of functions from this effort to the DOL and/or successor Contractor.

The Contractor shall be the lead on the transition activities during the transition period, leading Technical Exchange Meetings (TEMs) with the incoming Contractor to impart knowledge of the system(s) developed and activities performed under this effort, to include sustainment activities that are in progress. The TEMs shall include a demo of all components, the technology used, and a walkthrough of all documentation, to include the requirements backlog and the list of defects. The outgoing contractor shall allow for the incoming Contractor to ‘shadow’ them in obtaining knowledge of other aspects of contractual obligations other than what’s discussed during the TEMs. During this period, there shall be no degradation in support to the Government. At the COR designated turnover date (within the 30-day transition period), the successor Contractor shall assume full responsibility of the contract, while the outgoing Contractor focuses on contract closeout activities to complete the transition.

As part of the closeout activities, the Contractor shall confirm (in writing) that:

* DOL has received draft/in-progress and final versions of all documentation (e.g., CONOPS, SOPs, requirements specifications, design specifications, configuration management plan, etc.), to include the native format of diagrams (e.g., Visio), even those embedded in documents, have been uploaded into the DOL’s SharePoint project repository.
* DOL has received all GFE and GFI, e.g., PIV badges and laptops.
* DOL has received all source code, configurations, and database scripts.

The incumbent contractor shall present its plan for transitioning the services to the successor contractor to ensure continuity of services, minimize any decreases in productivity, and prevent negative impacts on additional services during the phase out period. This initiative will contain all items listed above as well as at minimum include:

* Points of contact
* Coordination with Government and contractor representatives to ensure a seamless transition
* Status of ongoing activities
* Schedules and milestones
* Actions required of DOL
* Orientation and documentation to explain the tools, methodologies, and processes used in this task order
* Transfer of technical and project management documentation including all system/tool documentation, code, and instructions required to operate, maintain and administer systems and tools
* Transfer of data, licenses, support contracts, and security codes, passwords, encryption keys, etc.
* Disposition of tool(s), services, and equipment used to support or test the provided services

Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management

# Part 6

## Applicable Publications

## 6.1 Publications Applicable to This PWS:

The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures as prescribed by Department of Labor (DOL) Office of the Chief Information (OCIO) and Office of the Assistant Secretary and Administration (OASAM) and applicable to this PWS. The Contractor shall also comply with IT security requirements in accordance with Federal and DOL regulations, policies, and procedures. Federal and industry standards applicable to this PWS include but are not limited to those listed below. The Contractor is further responsible for following the standards, codes, circulars, laws, directives, statutory requirements, regulations, standards, and guidance referenced within the cited publications.

From time-to-time Government standards will change and new related standards will be introduced. The Contractor shall ensure that it complies with the most current version of Government standards cited herein as well as changes to those standards and new related standards. If there are changes that significantly impact operations, the Government will work collaboratively with the Contractor to determine an expeditious approach for working through the technical, contractual, and/or cost implications, and implement the changes within a prescribed schedule.

## 6.1.1 Laws (Mandatory)

18 USC 1030, Fraud and Related Activity in Connection with Computers (dated 2002)

<https://www.govinfo.gov/content/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf>

18 USC 641, Public Money, Property or Records, Section 641 prescribes criminal penalties for misuse of any record, voucher, money, or item of value belonging to the United States or any department or agency of the Government. (Dated 2004) <https://www.govinfo.gov/content/pkg/USCODE-2021-title18/pdf/USCODE-2021-title18.pdf>

44 USC 3101, Records management by federal agencies (dated 2011)

<https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap31.pdf>

36 CFR Part 1228 - Disposition of Federal Records, Subpart L - Transfer of Records to the National Archives of the United States. (dated 2002)

<https://www.govinfo.gov/content/pkg/CFR-2000-title36-vol3/pdf/CFR-2000-title36-vol3-part1228.pdf>

PL 93-579 (5 USC 552a), the Privacy Act of 1974, as amended – (dated 1994)

<https://dpcld.defense.gov/Portals/49/Documents/Privacy/pa1974.pdf>

PL 107-347, E-Government Act of 2002 (dated 2002)

<https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

Plain Writing Act of 2010, <https://www.govinfo.gov/content/pkg/PLAW-111publ274/pdf/PLAW-111publ274.pdf>, (dated October 13, 2010) and resources on <https://www.plainlanguage.gov/>.

[21st Century Integrated Digital Experience Act (21st Century IDEA)](https://digital.gov/resources/21st-century-integrated-digital-experience-act/), December 2018

### 6.1.2 Federal Guidance (Mandatory)

NIST Cybersecurity Framework, <https://www.nist.gov/cyberframework> (dated 2018)

NIST Special Publications 800 Computer Security Series

NARA 2010-05, Guidance on Managing Records in Cloud Computing Environments (NARA

Bulletin) (dated 2010) <https://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html>

US Access Board Information and Communication Technology Revised 508 Standards and 255 Guidelines, <https://www.access-board.gov/ict/>(dated January 22, 2018). The [Section 508](https://www.section508.gov/) site provides guidance related to program management, procurement, tools and training, and policy compliance.

US Digital Services Playbook <https://playbook.cio.gov/> details 13 key practices from both the government and the private sector to help build focused and effective digital services.

[Checklist of Requirements for Federal Websites and Digital Services:](https://digital.gov/resources/checklist-of-requirements-for-federal-digital-services/) is a tool to access U.S. Government guidance and requirements in the development of websites and digital products.

[Research-based Web Design and Usability Guidelines - PDF](https://www.hhs.gov/sites/default/files/research-based-web-design-and-usability-guidelines_book.pdf) (21.9 MB) provides an overview of the user-centered design process and various UX disciplines. It also covers the related information on methodology and tools for making digital content more usable and useful.

[The U.S. Web Design System](https://designsystem.digital.gov/) offers open-source, quick-to-download code and assets, to make it easy to produce mobile-friendly and accessible government websites for the public. The site has guidance on the latest federal policy for websites and digital services.

Digital.gov provides a list of [Required Web Content and Links](https://digital.gov/resources/required-web-content-and-links/) that all federal websites need to have.

GSA Tech Guides <https://tech.gsa.gov/guides/#agile+api+design+development+devsecops+team>

[Style guides](https://digital.gov/resources/style-guides-by-government-agencies/) are used to set the tone and guidelines for how the agency communicates with the public.

[Policies, memos, circulars and executive orders](https://digital.gov/resources/omb-memos-circulars-executive-orders-and-other-policies/) released by the Office of Management and Budget (OMB) and other policies that are related to digital media and innovation.

The contractor shall be in full compliance with the AI Governance and development standards that are provided by various Executive Orders and regulatory guidance including:

* + [Executive Order 14110](https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence) (October 30, 2023)
  + [Executive Order 13960](https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government) (December 2020)
  + [Executive Order 13859](https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence) (February 2019)
  + [OMB M-24-10](https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf) (March 28, 2024)
  + [OMB M-21-06](https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf) (November 2020)

### 6.1.3 Industry standards (Advisory)

Agile Alliance, The Agile Manifesto, <https://agilemanifesto.org/> (dated 2001)

Industry Implementation of International Standard (ISO/IEC 12207-2017) Systems and Software Engineering- Software Life Cycle Processes – (dated 2017) <https://standards.ieee.org/ieee/12207/5672/>

SEI CMMI, Software Engineering Institute Capability Maturity Model Integration (dated March 2018) <https://cmmiinstitute.com/products/cmmi/dev> (Version 2.0)

Official Internet Protocol Standards, <https://www.rfc-editor.org/standards>

### 6.1.4 DOL specific standards, policies, and procedures (Advisory)

Below is a summary of relevant standards, policies, and procedures. This list may change over time at the Government’s discretion:

* 1. Systems Development Life Cycle Manual (SDLCM)
  2. Production Release Process
  3. Enterprise Architecture (EA)
  4. Cybersecurity Policy Portfolio (CPP)
  5. Section 508 Policy
  6. Digital Government Strategy
  7. Mobile Device Management (MDM)

# Part 7

## Technical Exhibit Index

1. Technical Exhibit 1 – Performance Requirements Summary
2. Technical Exhibit 2 – Deliverables Schedule
3. Technical Exhibit 3 – High Level Requirements

# Technical Exhibit 1

## Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. The performance objectives for this order are all the applicable Business Applications Services (BAS) Performance Requirements listed in the table below.

A monthly performance assessment will be completed by the IT Federal Project/Program Manager (IT FPM) and the COR to ensure that Contractor performance meets the established performance requirements as defined in the QASP. The quality measures reported by the Contractor in compliance with the QASP will be verified and validated by the IT FPM, and then a rating will be assigned.

Once the PRS ratings have been established, the document will be sent to the Contractor Program Manager (CPM) for review. The IT FPM, COR, and CPM will meet on a monthly basis to discuss these ratings, and also discuss and document any issues or concerns raised by either party. Additional Federal and Contractor personnel involved in the contract may attend the monthly meetings. Additionally, the CPM will meet with the COR on a regular basis (weekly, monthly, or as deemed necessary by either party). These meetings will provide a management-level review and assessment of the Contractor’s performance. When necessary, the CPM will provide a root-case assessment of failures, as well as the status of the corrective action taken.

| **BAS Performance Requirements (New Development as well as Operations and Maintenance)** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **SDLC Phase** | **Sub-Category** | **Requirement** | **Quality Standard** | **Performance Threshold** | **Method of Surveillance all coordinated with the COR** |
| 1 | Requirements | Develop agile story map (Product Roadmap) for the current release | Establish Story Map of the functionality for first production release (MVP) | Product Roadmap (Agile Story Map) that clearly describes all MVP components and features requested by the Product Owner and further indicates those that are capable of being delivered within the ceiling of this contract | Story map includes all functional, non-functional, security, authentication & authorization and 508 compliance epics. Complete roadmap delivered within 45 days of the contract award | Federal IT Project Manager review, Product Owner feedback (100 Percent Inspection). |
| 2 | Requirements | Develop and maintain agile story map for the current release | Story Map that provides a high-level visualization of the components and features requested by the Product Owner and further indicates those that are capable of being delivered within the ceiling of this contract. Maintain any changes thereafter throughout the period of performance | Complete story map that provides a high-level visualization of the components and features requested by the Product Owner and deliverables within the ceiling of this contract | Complete and accurate Product Roadmap delivered within 45 calendar days of award. No more than one reminder per every six months about keeping the story map up to date. | Review and approval of the Roadmap by the Federal IT Project Manager (100 Percent Inspection). |
| 3 | Requirements | Build and refine Product Backlog | Build the initial product backlog from the Agile story map. Continually refine the backlog to elaborate and write user stories. | Rolling wave planning should keep up with the development velocity. User stories must have accurate acceptance criteria | Refine continually. Critical acceptance criteria should not be missing from the user stories. 100% adherence to this requirement. | Review of rework as a result of inaccurate acceptance criteria. User story throughput prior to sprint planning (Periodic Surveillance) |
| 4 | Development-Sprint | Estimate the story map - Minimum Viable Product | Review story map and estimate the Epics | The story map should include high-level Agile point estimates (using 1 pt. = 8 hrs. LOE scale) related to developing and testing the components and features. | MVP Epics are estimated within 45 days of the contract award. | Review of the backlog by the Federal IT Project Manager (100 Percent Inspection). |
| 5 | Development-Sprint | Sprint Backlog | Sprint Backlog that is clearly linked to the story map and is further defined by User stories.  The backlog must be organized into Sprints and releases and includes story point estimates that correlate to the story map | Sprint backlog that is complete and accurate and includes Sprint planning at least three Sprints into the future | Accurate sprint backlog maintained for 3 sprints at a minimum | Review and approval of the Product Backlog by the Federal IT Project Manager. Feedback from the Product owner (Periodic Surveillance). |
| 6 | Development-Sprint | Sprit Planning | Analyze prioritized user stories and ensure that the acceptance criteria is understood and clarified ahead of a sprint for the next sprint. Perform detailed design of the story implementation. | User story should be fully understood and thought given to detailed design/implementation of the story | No critical defects due to misunderstood acceptance criteria. No major issues with the implementation | Customer testing feedback, government IT PM feedback, and JIRA report of defects. Architect review of the technical approach (Periodic Surveillance). |
| 7 | Development- Sprint | Sprit Planning | Select the features to be developed based on the capacity of the team and establish task list in the DOL hosted JIRA environment. | Number of stories selected are comparable with the capacity of the team. OCIO required Jira fields should be used/populated | Comparison of capacity vs work undertaken in each sprint. Maintain expected velocity. +/- 5% variability for a release. | Comparison of expected points for a sprint vs actual points completed (100 Percent Inspection). |
| 8 | Development- Sprint | Agile Tool Usage | Ensure that the JIRA is populated with the OCIO standard fields for each type of the entry. Use 1 point = 8hr LOE for allocating points. Use OCIO hosted central JIRA instance. Each JIRA field must utilize the same standards or status allocations as outlined by the OCIO guidelines. | DOL required Jira fields should be populated and used according to the OCIO usage guidelines of story status and defect categorization. Traceability between Epics, stories and tasks/ defect etc. clearly maintained. | Review of PPM dashboard and Jira data entry. No more than one reminder per quarter | Jira fields review and PPM dashboards (Periodic Surveillance) |
| 9 | Development- Sprint | Sprint Execution | Deliver agreed-to functionality for the monthly sprint throughout the duration of the project, ensuring required artifacts are produced for each release and the quality of the work is within acceptable standards | Functionality delivered in the sprint reflects discussed and documented acceptance criteria provided by the Government for each approved user story assigned to the current sprint | Completes 95% of tasks according to the project schedule. +/- 5% variability for a release. | Schedule variance - actual vs baseline (100 Percent Inspection). |
| 10 | Development- Sprint | Sprint Execution | Deliver agreed-to functionality for the monthly sprint throughout the duration of the project, ensuring required artifacts are produced for each release and the quality of the work is within acceptable standards | Functionality delivered in the sprint reflects discussed and documented acceptance criteria provided by the Government for each approved user story assigned to the current sprint | Ensure developer performs unit testing against the acceptance criteria resulting in 95% error free on new functionality, and 100% error free for defects fixed from the previous iterations' build | Federal IT PM review of number of failed acceptance criteria per story. JIAR defect report (100 Percent Inspection). |
| 11 | Development- Sprint | Sprint Execution | Execute and document code review for each sprint in additional to static code analysis results as applicable | For each sprint, for each team, document code review results and provide to the federal architect | Ensure that one code review, per team, is performed every sprint | Review of the report by federal architect (Periodic Surveillance). |
| 12 | Development- Sprint | Traceability | Defects that are found and reported during acceptance testing shall be tracked and categorized.  The defects shall be categorized as per OCIO defines categories. Also, every defect entered must have linkage to the user stories. (Roadmap –User Stories – Tasks – Defects/issues) | End-to-end defect tracking that is complete and accurate and is provided at the end of every testing cycle. | No more than one reminder for missing traceability | Jira and PPM tool reports (Random Sampling) |
| 13 | Development- Sprint | Sprint Velocity | Development of features shall proceed at the rate described during baselining, with acceptable deviation. Implement features according to agree upon product story map. | All essential features are implemented and working as specified in user stories and other requirements by agreed upon schedule. Accrued velocity beginning at a frequency equivalent to three (3) Sprints shall be within acceptable deviation. | Accrued development velocity shall not have a negative deviation of more than 5%. Points are earned after a user story is developed and passes system testing, not just by LOE without outcome. | Review and approval of the Burn up Chart by the Federal IT Project Manager (100 Percent Inspection). |
| 14 | Development- Sprint | 508 Compliance | System to be developed in accordance with the DOL Section 508 Program Office guidelines. | Ensure accessibility is considered at all phases of product and service delivery in accordance with departmental guidelines and reflected in each sprint. Use OCIO required tools to test 508 compliances. | Web Content Accessibility Guidelines 2.1 AA standards much be followed for each sprint. Must pass the core 508 requirements 100% | <https://labornet.dol.gov/itc/it/Section508/>  (Periodic Surveillance) |
| 15 | Development- Sprint | Documentation | Ensure all project artifacts are properly documented for each sprint | All dependencies are listed, and the licenses are documented. Major functionality in the software/source code is documented. Individual methods are documented inline in a format that permit the use of tools such as Judo. System diagram is provided. | No more than 1 reminder per quarter. Combination of manual review and automated testing, if available | Federal architect or IT PM review (Periodic Surveillance) |
| 16 | Development- Sprint | Sprint -Review | Burn “up” chart that is directly derived from the Roadmap, Product Backlog, and velocity estimates provided by the contractor.  The chart must include the baseline scope, actual scope, baseline velocity, planned velocity, and actual velocity. | Burn “up” chart that is complete and accurate and is provided at the end of every Sprint | Burn “up” chart that is complete and accurate and is provided at the end of every Sprint 100% of the time | Review and approval of the Product Backlog and planned and actual development velocity by the Federal IT Project Manager (100 Percent Inspection). |
| 17 | Development- Sprint | Sprint Deployment | Follow DOL configuration procedures and Change Management practices. Ensure that the release builds are deployed without issues. | Follow DOL procedures and standards. | No issues with production deployments. No more than minor issue with other deployments. | Federal IT PM review (Periodic Surveillance) |
| 18 | Development- Sprint | Security | Deliver secure products including background investigations and other practices even if Contractor’s staff are not physically accessing DOL facilities and requesting accounts on the DOL network. Contractor staff who are developing/maintaining/operating DOL systems on external Cloud and on-premise platforms still need to meet this requirement | Security requirements are clearly followed (including any special considerations related to the particular work, ex. working with SSN’s, health information, etc.) | Complete and thorough adherence to security requirements | Review by the OCIO security team and federal IT PM (Periodic Surveillance) |
| 19 | Development- Sprint | Solution Architecture and Product Decisions | Obtain written Government approval for architecture and product decisions used to develop, operate, and maintain the product. | Written Government approval is required for architecture and product decisions used to develop, operate, and maintain the product. | 100% Conformance with the Government's architecture and approved products. | Review and approval by the Federal IT Project Manager and the federal architect (100 Percent Inspection). |
| 20 | Development- Sprint | Coding standards and Best practices | Relevant Industry coding standards and best practices are implemented all the time | At minimum general OCIO development guidelines are followed and implemented to ensure code quality (readability, maintainability, reusability & lower technical debt) | There should be no more than 10% of code quality variation from OCIO defined code development guidelines | Federal architect review (Periodic Surveillance). |
| 21 | Development- Sprint | Performance Testing | Performance testing or response time testing to be performed for newly developed medium & major features | Ensure OCIO performance service level agreements (SLAs) are met and also following metrics are captured but not limited to: speed, response times, latencies resource usage etc. | The system and related sub systems behaves and responds properly as per OCIO SLA under high demand or during its peak usage. | Federal architect or IT PM review (100 Percent Inspection). |
| 22 | Development- Sprint | User Experience (UX) | Use UI/UX/Accessibility Standards and Best Practices so that all user-facing elements conform to the 21st Century IDEA | Ensure that all user-facing elements (mobile / web / client-side app / etc.) adhere to the act known as the 21st Century IDEA. | There should be no more than 20% of code that produces elements not aligned with IDEA. | Federal architect review (Periodic Surveillance). |
| 23 | Ownership | Government Insight | Ensure that the Government has full insight into requirements tracking, testing, defects, application helpdesk, and overall product delivery. | Ensure the Government have full access to all environments, Jira, CM, helpdesk, and similar product instances. | 100% Government full access is provided and maintained for all Jira, CM, helpdesk, and similar product instances. | Review and approval by the Federal IT Project Manager (100 Percent Inspection). |
| 24 | Ownership | Government Code Repository | Ensure that all system code is maintained in the Government’s code repository and that the Government has full access to the latest production code and code that has been under substantial development at all times. | Ensure the Government has full access to the latest production code and code that has been under substantial development at all times | 100% Government full access is provided and maintained for the latest production code and code that has been under substantial development at all times. | Review and approval by the Federal Project Manager (100 Percent Inspection). |
| 25 | Contract Transition | Contractor Transition Out | Incumbent Contractor to perform detailed knowledge transfer including shadow production operation If a different Contractor is selected. | Ensure the incoming Contractor is provided detailed knowledge transfer including shadow operation if a difference Contractor is selected | 100% detailed knowledge transfer including shadow operation is provided in case Contractor turnover. | Review and approval by the Federal Project Manager (100 Percent Inspection). |
| 26 | Production Support | Issue Resolution | Production support tickets received by the Contractor must be responded to promptly based on the severity of the issue reported. Ensure that repeat issues are minimized. | Follow SLA agreed with OCIO | No more than one reminder for missing timeliness per every six months. No repetition of already reported issue that is expected to have been resolved the first occurrence. | Government IT Project manager and JIRA issue report (Periodic Surveillance). |
| 27 | Communications | Contractor Support and Escalation Contact List | Maintain and provide to the Government on at least a quarterly basis a support and escalation contact list. | Ensure the Government is provided a well-maintained support and escalation contact list related to any service components at least on a quarterly basis. | Government is provided a well-maintained list of support and escalation contact list on at least a quarterly basis 100% of the time. | Review and approval by the Federal IT Project Manager (Periodic Surveillance). |
| 28 | Communications | Project status and cost, schedule, scope discussions | Contractor to work with the Federal IT PM while handling project status discussions with the end customers. | Follow established communication protocols. Ensure that the Federal PM approves the communication. | No more than one reminder per quarter. | Review and approval by the Federal IT Project Manager (100 Percent Inspection). |
| 29 | Service Level | Unscheduled Service Interruptions | Monitor operational systems and provide timely notification for any unscheduled service interruptions (USI’s). | Ensure customers are notified of any unscheduled service interruptions in a timely manner. | Notify the Government customers of any unscheduled service interruptions as soon as possible and no later than 30 minutes after the incident. | Review and approval by the Federal IT Project Manager (Periodic Surveillance). |
| 30 | Maintenance of the system | Keep Maintenance Product Current | Maintain currency of any products used to operate/maintain systems (ex. keep Oracle up-to-date, Java JRE, etc.) | Ensure all products used to operate/maintain systems are kept current according to the OCIO schedule of deployments. | Product used to operate/maintain system are kept current 100% of the time | Review and approval by the Federal IT Project Manager (Periodic Surveillance). |
| 31 | Security Posture | Security Scan | Perform security scan using Government recommended tool and obtain approval from DOL security team | Ensure security scan is performed based on requirements from the Government and approval from DOL security team is obtained to meet deadline. | Security scan is performance including corrective actions fulfilment and approval is obtained from the DOL security team 100% if time. | Review and approval by the Federal IT Project Manager (100 Percent Inspection). |

# Technical Exhibit 2

## Deliverables Schedule

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PWS Section 5 Task** | **Deliverable** | **Due** | **Format** | **Submit To** |
| Transition In | Contractor personnel suitability (e.g., background investigation) packages | 14 calendar days from award | Resume, PIC, OF-306, and eQIP | COR |
| Transition In | Task Order Management Plan | 21 calendar days from award | PDF | COR and Federal Project Manager |
| All | Quality Control Plan | 60 calendar days after award | Word | Federal Project Manager |
| All | Monthly status report (accomplishments, planned, risks/issues with mitigation strategies) | Monthly | Word or PowerPoint | COR and Federal Project Manager |
| All | Monthly invoices | Monthly | TBD | COR |
| All | Contractor personnel suitability (e.g., background investigation) packages  for staff changes | 30 calendar days prior to desired onboarding | Resume, PIC, OF-306, and eQIP | COR |
| All | Configuration Management Plan | 60 calendar days after award | Word | Federal Project Manager |
| Operations | Root cause analysis for all unplanned production outages | 7 calendar days after restored | Word/ PowerPoint | Federal Project Manager |
| Operations | Updated Jira bug tickets for user reported issues through fix being deployed in production | End of Sprint and Deployments | Jira | Jira |
| Operations | Refresh plan including COTS End Of Life impacts | Annually | Word | Federal Project Manager |
| Maintenance | Plan (Epics/User Stories) to address maintenance needs with high level estimates | 14 calendar days after request | Jira | Federal Project Manager |
| Maintenance | Updated Jira User Stories through being deployed in production | End of Sprint and Deployments | Jira | Jira |
| Maintenance | Test plan for each release specifying test approach and success criteria, including but not limited to Section 508 WCAG elements | 5 calendar days after Sprint start | TBD | COR and Federal Project Manager |
| DME | Plan (Epics/User Stories) to address significant LOE with high level estimates | 14 calendar days after request | Jira | Jira |
| DME | Updated Jira User Stories for smaller LOE efforts through being deployed in production | End of Sprint and Deployments | Jira | Jira |
| DME | Detailed System Design, Data, and Interface documentation | 90 calendar days after award, then updated as needed | Word/Excel | Federal Project Manager |
| DME | User training material (e.g., manuals, aids, videos) | 30 days prior to desired release | TBD | Federal Project Manager |
| DME | Results report for each Sprint | 1 calendar day after Sprint end | Codebase/PDF, test report(s), demo of product increment, sprint performance metrics | Federal Project Manager |
| DME | Updated Product Backlog | 1 calendar days after Sprint start | Jira | Jira |
| Transition Out | Transition plan | 60 calendar days before project end | Word/PDF | COR and Federal Project Manager |
| Transition Out | Finalized implementation and support documents | 30 calendar days before project end | Source/PDF | COR and Federal Project Manage |
| Transition Out | Source code, configurations, etc. | 30 calendar days before project end | Gitlab | COR and Federal Project Manager |
| Transition Out | List of government provided GFE returned and accepted | Upon project end | Word/Excel | COR and Federal Project Manager |

In order to meet Section 508 accessibility requirements for all technology procured, maintained, developed or used by the Contractor at, or on behalf of, DOL – to include electronic documents, software, websites and webpages created or maintained by the Contractor and the deliverables listed above – the Contractor shall:

1. Provide summary narrative text descriptions or a data table describing each complex graphic (e.g., pie graphs, line graphs, maps, bar graphs, flow charts) in a separate comma-separated values/character-separated values (CSV) file.
2. Label each figure or graphic image with an alternate text description.
3. Ensure Contractor support staff producing ICT deliverables have a solid working knowledge of Section 508 and can perform Quality Assurance Testing for Section 508 and the applicable WCAG success criteria. Verification of such knowledge shall be provided for the individuals proposed on the contract.
4. Have updated authoring and testing tools to produce Section 508 output on their own. (The Government will not provide these tools.)
5. Provide two digital copies of any report over 25 pages in media formats readable by Windows-based programs; one copy formatted in Microsoft Word and the second in the Portable Document Format (PDF). Color and/or black & white PDFs are acceptable. Reports shall not be submitted in HTML format, unless specifically requested.

The Section 508 Standards described herein provide the minimum Government requirements and do not, in any way, diminish the Contractor’s responsibility to meet additional requirements that may be applicable under the law. Additional information about accessibility standards related to Section 508 may be found at: <http://section508.gov/>

Additional information about creating accessible PDF files may be found at: <http://www.section508.gov/docs/pdfguidanceforgovernment.pdf>

## Electronic Records Management

* + Continued technological and project management support of the DOL Electronic Records Management System (eRMS) and Metadata/Taxonomy for electronic records management
  + Meetings and project management support for a litigation hold system
  + Future Enterprise Digitization/Scanning of paper/analog records
  + Continue to align records management strategic goals with OCIO to meet M-23-07
  + IT Modernization and Information Governance goals as aligned with records management strategic plan
  + Records Management for All and Controlled Unclassified Information (CUI) training in Learning Link
  + Support in intranet site redesign for Records Management pages
  + Manage DOL contract for the design, development and implementation of the Electronic Records Management Platform
  + DOL baseline taxonomy

# Technical Exhibit 3

### Task Area 1: Artificial Intelligence

Contractor must provide AI Implementation Services which includes Use case discovery, ideation, proof of concept/proof of value, development, deployment, production, operation and maintenance O&M, monitoring. The AI implementation services which include products and solutions will be designed to seamlessly integrate, develop, and government and industry practices across the DOL IT portfolio of applications.

The AI activities are inclusive and not limited to designing, delivering, and supporting custom models, and using GEN AI technologies to develop enterprise services, capabilities, applications, and utilities using CSPs, COTS  products, and Open Source and by integrating AI custom models into existing applications and services, extending the solution to enhance Generative AI use cases, and leveraging established AI technologies and principles such as data preprocessing, feature engineering, model training, and model evaluations. The desired outcome is a future-proof framework/capability/process that is efficient, extensible, future-proofed, and tailored to the needs of the DOL.

The Contractor must create a model factory and a model marketplace to facilitate the deployment and management of AI models as required.

The AI solution delivery must using enterprise agile in compliance with all DOL OCIO IT/AI/Data/Security/ Agile requirements and guidelines which are based on public sector AI/IT requirements such as WH Exec Order, OMB, NIST Risk Management Framework and are also based on industry best practices, standards, and frameworks such as Agile, CRISP-DM (Cross-Industry Standard Process for Data Mining), and TDSP (Team Data Science Process). The Contractor will collaborate with stakeholders to identify business needs, gather requirements, and prioritize features aligned with strategic goals. The AI solution will be scalable enterprise wide, extensible, and adaptable to accommodate evolving business needs and emerging technologies.

### Task Area 2: Enterprise Engineering and Architecture

The Contractor shall provide architecture and engineering service support for the following:

Enterprise Architecture: Expertise to abide by and help develop DOL’s Strategic Roadmap in support of ensuring OCIO technology strategy serves their business strategy by:

* Maintaining Governance awareness of larger Federal initiatives and policy
* Developing, managing and maintaining an OCIO Service portfolio
* Assessing the current as-is state and recommending Future state for each OCIO service as well as incremental plan to achieve this state.
* Work with other DOL divisions to Developing the enterprise-wide standards and reference architectures to guide IT delivery.
* Discovery and Inventory: This task will consist of conducting an automated inventory of the as-is state of DOL’s environment.
* Facilitate the creation of a Business Capability Model
* Maintain IT Data Model roadmap.
* Develop New software intake process
* Support OMB and internal Data calls
* Manage the Reference Architecture
* Support IT Modernization
* Mange the IT Modernization Score card
* Facilitate Cross Functional expertise in the ITARB evaluations.
* Working with AE and TIE SORT team provide solutions Design.
* Develop and review policies and processes in supporting the DOL enterprise architecture program and any projects within IT system Engineering and Integration Support services.
* Design, develop and/or peer-review architectures, and conduct implementations for engineering projects at DOL .
* Support platform infrastructure associated with AI/ML and Robotic Process Automation initiatives.
* Intake and assessment of agency Demands/use cases
* Develop and review policies and processes supporting TIE
* Supports establishing DOL-wide ERM standards and governance.
* Provide engineering support to the ERM team

**Task Area 3: Mobile Application Development**

The contractor shall provide services for Mobile App Development. The contractor shall be able to adapt and provide the necessary resources (project management, business analysis, design, and development) to maintain minimum throughput and work in progress (WIP) service levels agreed to between OCIO and its customers.

The maintenance and development support includes the following major areas:

* Project Management
* Mobile Application Design, Development, Testing, and Support

### Task Area 4: Emerging Technology

Contractor services needed for Emergency Technology task area are inclusive and not limited to Quantum Computing including activities related to post quantum crypto readiness and quantum algorithms, support for innovative technologies such as Augmented Reality & Generative AI, ability to evaluate and bring in new technologies and services to the DOL ecosystem as required by DOL**.**

**Task Area 5: Security Solutions**

Contractor services needed for Security Solutions task area are inclusive and not limited to implementing:

* Establishing measurable security risk management frameworks compliant with federal standards such as NIST RMF, NIST AI RMF, and all Office of the Chief AI Office (OCAIO), Chief Technology Officer (CTO), DOL requirements.
* Implementing and managing enterprise security tools, solutions, processes, and monitoring.
* Ensuring security for all AI systems using measurable and repeatable processes.
* All Post Quantum Crypto (PQC) readiness activities including developing approaches and supporting DOL’s platforms, applications, tools, data, information, and services for PQC safety.

### Task Area 6: Electronics Records Management

* Continued technological and project management support of DOL Electronic Records Management System (eRMS) and Metadata/Taxonomy for electronic records management
* Meetings and project management support for a litigation hold system
* Future Enterprise Digitization/Scanning of paper/analog records
* Continue to align records management strategic goals with OCIO to meet M-23-07
* IT Modernization and Information Governance goals as aligned with records management strategic plan
* Records Management for All and Controlled Unclassified Information (CUI) training in Learning Link
* Support in intranet site redesign for Records Management pages
* Manage DOL contract for the design, development and implementation of the Electronic Records Management Platform
* DOL baseline taxonomy