REQUEST FOR QUOTATION
(THIS IS NOT AN ORDER)

THIS RFQ [X] IS [ ] IS NOT A SMALL BUSINESS SET-ASIDE

PAGE 1 OF PAGES 48

1. REQUEST NUMBER	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NUMBER	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG. 1	RATING
1605TA-25-Q-00039	06/27/2025			

5a. ISSUED BY
US Department of Labor
Customer Acquisition Services
200 Constitution Ave, NW
S-4307
Washington DC 20210

6. DELIVER BY *(Date)*: Multiple

7. DELIVERY: [X] FOB DESTINATION [ ] OTHER *(See Schedule)*

5b. FOR INFORMATION CALL *(NO COLLECT CALLS)*

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
Marlon Chambers	202	693-6523

9. DESTINATION

a. NAME OF CONSIGNEE: US DEPARTMENT OF LABOR

8. TO:

a. NAME

b. COMPANY

c. STREET ADDRESS

b. STREET ADDRESS: 200 CONSTITUTION AVE., NW N4123

c. CITY: WASHINGTON

d. CITY	e. STATE	f. ZIP CODE	d. STATE	e. ZIP CODE
			DC	20210

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS *(Date)*: 07/03/2025 04:00 P.M. ET

IMPORTANT: This is a request for information and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or service. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotation must be completed by the quoter.

11. SCHEDULE *(Include applicable Federal, State and local taxes)*

ITEM NUMBER (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	The U.S. Department of Labor (DOL), Office of the Senior Procurement Executive (OSPE), on behalf of the Office of the Chief Information Officer (OCIO), is issuing this 8(a) sole-source solicitation to provide Youth Build (YB) and Division of Indian Native American Program (DINAP) case management system support services in accordance with the Performance Work Statement(PWS) and SBA Requirement# FT1746025704M. The government anticipates award of a Labor-Hour contract. The period of performance (POP) for the Continued...				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations [ ] are [ ] are not attached.

13. NAME AND ADDRESS OF QUOTER	14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION	15. DATE OF QUOTATION
a. NAME OF QUOTER		
b. STREET ADDRESS	16. SIGNER	
	a. NAME *(Type or print)*	b. TELEPHONE AREA CODE
c. COUNTY		
d. CITY / e. STATE / f. ZIP CODE	c. TITLE *(Type or print)*	NUMBER

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6/1995)
Prescribed by GSA-FAR (48 CFR) 53.215-1(a)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	resultant contract will be for 12 months from the date of award with three (3), 12-month option periods. Clarifying questions are due by Tuesday July 1, 2025, at 4:00pm ET via email to Marlon Chambers, Contract Specialist, at chambers.marlon.k@dol.gov, with CC to Jermaine Duncan, Contracting Officer, at duncan.jermaine.l@dol.gov. The subject line of the email shall contain the solicitation number. The Government will not accept or respond to questions posed via telephone. The quote must be signed by an authorized representative of the company and submitted no later than the date and time specified in block 10 of this SF 18. The quote shall be submitted via email to Marlon Chambers, chambers.marlon.k@dol.gov, with a copy to Jermaine Duncan, duncan.jermaine.l@dol.gov. ANY DISCOUNTS ARE HIGHLY ENCOURAGED. Period of Performance: 07/11/2025 to 07/10/2029				
0001	Base- Youth Build (YB) and Division of Indian Native American Program (DINAP) Case Management System Support Services Product/Service Code: DA01				
1001	OP1- Youth Build (YB) and Division of Indian Native American Program (DINAP) Case Management System Support Services (Option Line Item) (Anticipated Option Exercise Date) 06/10/2026 Product/Service Code: DA01				
2001	OP2- Youth Build (YB) and Division of Indian Native American Program (DINAP) Case Management System Support Services (Option Line Item) (Anticipated Option Exercise Date) 06/10/2027 Product/Service Code: DA01				
3001	OP3- Youth Build (YB) and Division of Indian Continued...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Native American Program (DINAP) Case Management System Support Services (Option Line Item) (Anticipated Option Exercise Date) 06/10/2028 Product/Service Code: DA01				

B - Supplies or Services/Prices

CLIN	DESCRIPTION OF WORK	QUANTITY/HOURS	UNIT	UNIT PRICE	TOTAL
0001 - Base	Labor	1	LO	----	
	01- Requirements Analyst/Business Analyst (Key)	1912	HR		
	02- Senior Level Appian Developer (Key)	1912	HR		
	03- Mid-Level Appian Develop	1912	HR		
1001 - OP 1	Labor	1	LO		
	01- Requirements Analyst/Business Analyst (Key)	1912	HR		
	02- Senior Level Appian Developer (Key)	1912	HR		
	03- Mid-Level Appian Develop	1912	HR		
2001 - OP 2	Labor	1	LO		
	01- Requirements Analyst/Business Analyst (Key)	1912	HR		
	02- Senior Level Appian Developer (Key)	956	HR		
	03- Mid-Level Appian Develop	1912	HR		
3001 - OP 3	Labor	1	LO		
	01- Requirements Analyst/Business Analyst (Key)	1912	HR		
	02- Senior Level Appian Developer (Key)	956	HR		
	03- Mid-Level Appian Develop	1912	HR		
	GRAND TOTAL				

C - Description/Specifications

Performance Work Statement for Youth Build (YB) and Division of Indian Native American Program (DINAP) Case Management System Support Services

PART 1 GENERAL INFORMATION

The Grants Management Directorate of Business Application Services Directorate under the Office of the Chief Information Officer, OCIO, would like to maintain the existing case management system GPMS YB-DINAP Appian production system. 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 tasks defined herein. The existing case management system Youth Build (YB) and Division of Native American Program (DINAP) is built upon the Appian Department of Labor, Department of Labor (DOL), Platform. The vendor will utilize to the maximum extent possible, utilize the GPMS YB-DINAP system platforms' existing code, configurations, workflows, data schema, etc. to maintain and further develop these systems. This includes Appian front end development, back-end Oracle Amazon Web Services, AWS, database management/development, cloud server configuration for each environment (minimally Development, Test, Stage, Training, and Production), management of electronic storage, and all work necessary to maintain the existing YB and DINAP systems.

1.1. Description of Services/Introduction:

The contractor shall provide all personnel, equipment, tools, materials, supervision, and other items and non-personal services necessary to perform services, as defined in this Performance Work Statement, except as Specified in Part 3 as government furnished property and services. The contractor shall perform to the standards in this contract.

1.2. Background:

Indian and Native American (INA) Workforce Innovation and Opportunity Act (WIOA) Section 166 grantees and the Department of Labor share a vision of providing quality employment and training services to Native American communities that not only meet regulatory requirements, but also are administered in ways that are consistent with the traditional cultural values and beliefs of the people they are designed to serve.

The YB and DINAP applications are part of a larger Grantee Performance Management System, centralizing configuration as much as possible and reducing duplicity among systems. These systems also share a common back-end system and real-time PIRL compliant items. Further, GPMS integrates with the Workforce Integration Performance System, WIPS, which produces each programs quarterly performance reports.

For more information about the DINAP program, please visit the DINAP website at https://www.dol.gov/agencies/eta/dinap
https://www.dol.gov/agencies/eta/dinap
For more information about the Youth Build program, please visit the Youth Build website at
https://www.dol.gov/agencies/eta/youth/youthbuild

1.3. Objectives:

The objective of this PWS is for a Contractor to provide services to perform requirements gathering and planning as well as configuration, development, test, and implementation of a case management solution for the ETA YB-DINAP system. The Government requires this solution to be implemented on the DOL Appian Cloud. This involves requirements to leverage reuse of existing components as appropriate.

The main objectives of this task order are to:

- Provide Operations and Maintenance, O&M, support for the system.
- During the analysis phase the contractor will document the business processes, conditions of validation, procedures, and the functional specifications.

1.4. Scope:

The scope of this Performance Work Statement is to ensure the vendor provides O&M services to YB-DINAP production system and gather requirements, plan, develop, test, implement and the Oracle database located in the DOL Amazon Web Services, AWS, cloud. The case management system will be part of DOL's Appian Cloud platform developed to meet the long-term GPMS YBDINAP. The scope includes configurable workflows, reporting, functional reusability, ability to integrate with existing other DOL APPIAN systems and data, ability to handle multiple programs and case management flows, ability to handle various reporting needs, and ability to integrate with future DOL Information Technology, IT, Platform OCIO data architecture. The broader scope of the project involves utilizing the configuration of the existing platform and building upon the GPMS YB-DINAP Appian system per customer requirements, while supporting the unique needs and workflow requirements as detailed by customer requirements.

The contractor shall work collaboratively with the Government to adjust the scope of each Epic to ensure the project stays within the budget and schedule constraints.

Please see Part 5 Specific Tasks as well as **Technical Exhibit 3 Requirements**

1.4.1 Architecture Restrictions:

The solution proposed by the vendor for the system shall meet the below listed restrictions:

- The vendor will take, inherit as-is the WIPS system as hosted in Appian SAAS environment and DOL's AWS cloud platform.
- Any changes to the WIPS environment should be within the constructs of OCIO Cloud environmental specifications
- All new/upgraded services shall be stood up on DOL's Appian Cloud platform unless it is prohibitively expensive to do so and approved by the federal program manager and COR.
- Any upgrades to address retirement of a service by the AWS cloud vendor should be planned, approved by OCIO federal management team, and completed 45 days before the retirement of said service.

1.5. Period of Performance:

The period of performance shall be for one (1) 12-month base period and three (3) 12month option periods. The period of performance reads as follows:

Performance Period	Estimated POP
Base Period	07/11/2025 to 07/10/2026
Option Period 1	07/11/2026 to 07/10/2027
Option Period 2	07/11/2027 to 07/10/2028
Option Period 3	07/11/2028 to 07/10/2029

The Government also reserves the right to extend the term of this contract at the prices set forth in Section B in accordance with the terms and conditions contained in FAR clause 52.217-9, "Option to Extend the Term of the Contract".

1.6. General Information

1.6.1. Quality Control (QC):

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". The Quality Control Plan should be submitted as part of the Contractor's technical proposal and may be included as an appendix to the proposal. After acceptance of the quality control plan, the contractor shall receive the contracting officer's acceptance in writing of any proposed changes to the quality control system.

QC is deliverable-oriented and focuses on measuring, testing and/or inspecting products and services. Though generally performed at different phases of the product life cycle, there is a specific focus on the final deliverable. The aim of QC is to ensure that all products and services meet the applicable design specifications and quality standards. The QC Team conducts audits of the quality monitoring for OCIO-provided products and services, as well as for products and services provided by Contractors to the OCIO.

For purposes of QC, the Contractor shall measure its performance based upon the processes and standards/metrics as developed in conjunction with the OCIO QA Team or the Contractor developed industry standard metrics, as defined in the QASP. Additionally, the Contractor shall cooperate fully with the OCIO QA Team during audits, including but not necessarily limited to (i) providing documentation and supporting details, and (i) conducting root cause analysis and corrective action planning activities, as established for the OCIO at large.

1.6.2. Quality Assurance (QA):

The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). 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).

QA focuses on eliminating process variation by creating, revising, and strictly implementing a set of tightly and precisely defined (1) processes, (2) procedures (tools), and (3) quality standards (review mechanisms) that, when exactly followed, ensure the final quality of the product or service.

The OCIO QA Team is involved in three general functions: Standards Definition, Process Audit, and Product Audit. The Contractor shall work with the OCIO QA Team to (i) define and establish appropriate standards/metrics for the work performed under this contract; (ii) document standardized processes in the form and format determined by the OCIO QA Team; and (iii) develop applicable audit processes that will support ongoing oversight by the OCIO QA Team. The Contractor shall respond to the OCIO QA Team according to the processes (including timing, method, and level of detail) as established for the OCIO at large.

In the event that the OCIO QA Team is delayed in working with the Contractor on the activities described above, then the Contractor shall establish interim industry standard metrics and begin active measurement in order to establish a performance baseline. These interim metrics shall be presented to the IT Federal Program Manager (FPM) and the COR for their approval prior to implementation.

The COR and the IT FPM will work with the QA Team to establish a Quality Assurance Surveillance Plan (QASP) that corresponds to the performance objectives and standards (i.e., quality, quantity, timeliness) specified in this Performance Work Statement (PWS). The QASP will provide specific details on how the Government will survey, observe, test, sample, evaluate, and document Contractor performance results to determine if the Contractor has met the required standards for each objective.

1.6.3. Section 508 Compliance:

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.

1.6.4. General Requirements:

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

Acceptance and Conformance

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).

1.6.5. Continuous Improvement:

The Branch of QM also houses the IT Continuous Process Improvement, CPI, Team. This function is responsible for monitoring, reviewing and modifying processes to improve IT service delivery, as well as the development and deployment of IT products. The CPI Team focuses on reducing costs, reducing risks and improving quality. The CPI Team uses the results of other QM functions to identify potential areas of improvement and develop appropriate solutions. The Contractor shall cooperate fully with any continuous improvement activity undertaken by the CPI Team where the Contractor is determined to be a stakeholder. Furthermore, the Contractor shall fully support the implementation of any process improvements identified by any CPI activity.

1.6.6. 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.

1.6.7. Recognized Holidays:

Designation of Holidays per OPM: https://www.opm.gov/policy-data-oversight/pay-leave/payadministration/fact-sheets/holidays-work-schedules-and-pay
https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.opm.gov%2Fpolicy-data-oversight%2Fpay-leave%2Fpay-administration%2Ffact-sheets%2Fholidays-work-schedules-and-pay&data=04%7C01%7CWickliffe.Larry%40dol.gov%7Ca258561a2c1148d0207f08d9922f9ed5%7C75a6305472044e0c9126adab971d4aca%7C0%7C0%7C637701555623675877%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=GoboqJHJ5jhjF95ov8sRgqXXzTFzxG53nBCFfhRnvxI%3D&reserved=0

New Year's Day	January 1
Martin Luther King Jr.'s Birthday	Third Monday in January

President’s Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	June 19
Independence Day	July 4
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11
Thanksgiving Day	Fourth Thursday in November
Christmas Day	December 25

1.6.8. Hours of Operation/Place of Performance:

The Contractor is responsible for conducting business between the hours of 6:00 a.m. and 8:00 p.m. Eastern Time, Monday through Friday, except during Government Recognized Holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. After-hours on-call support will be required for “emergency” (i.e., system outage) issues including weekend deployment support as well as during federal holidays support. After-hours support may be requested to support deployments or training sessions.

The Contractor shall not be reimbursed when the government facility is closed for the above reasons. The Contractor must, at all times, maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS (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 workforce are essential.

Telework for contractor employees may be authorized in accordance with the employer’s hiring policies.

When authorized, telework must be approved in writing in advance by the Contracting Officer's Representative, COR, and the Contracting Officer, CO, in accordance with the terms and conditions described in this section.
(a) Contractor employees authorized to telework will be provided DOL equipment, which includes a laptop, or other device provisioned by DOL for secure authenticated access. No other equipment is authorized for use when teleworking.
(b) 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.
(c) The Government will not provide or reimburse contractor employees for internet connectivity.

The work to be performed under this task order shall be performed at: 200 Constitution Avenue, NW, Washington, DC 20210.

Alternate Place of Performance - Contingency Only. As determined by the FPM in coordination with the COR and approval of the CO, Contractor employees may be required to work at an alternate place of performance (e.g., home, the Contractor's facility, or another approved activity within the local travel area) in cases of unforeseen conditions or contingencies (e.g., pandemic conditions, exercises, government closure due to inclement weather, etc.). Nonemergency/non-essential Contractor staff should not report to a closed government facility. Contractor shall prepare all deliverables and other contract documentation utilizing Contractor resources. To the extent possible, the Contractor shall use best efforts to provide the same level of support as stated in the Performance Work Statement (PWS). In the event the services are impacted, reduced, compromised, etc., the Contracting Officer or the Contractor may request an equitable adjustment pursuant to the Changes clause of the contract.

1.6.9. Type of Contract:

The government anticipates award of a Labor Hour Task Order.

1.6.10. Security Requirements:

Individual contractors on task with this order may be required to submit information for security and background prescreening sufficient to meet Homeland Security Presidential Directive 12 (HSPD-12) requirements. Software developed in accordance with Secure Software Development standard and the attestation form provided with each delivery.

Physical Security.
The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

Key Control.
The Contractor shall establish and implement methods of making sure all
Keys/key cards issued to the Contractor 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 Contractor by the Government shall be duplicated. The Contractor 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 Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

Lost Keys
In the event keys, other than master keys, are lost or duplicated, the Contractor 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 Contractor. 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 Contractor.

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

Lock Combinations.
The Contractor shall establish and implement methods of ensuring that not all lock combinations are revealed to unauthorized persons. The Contractor 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 Contractor's Quality Control Plan.

Conservation of Utilities.
The contractor shall instruct employees in utilities conservation practices. The contractor 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.

1.6.11. Cybersecurity Requirements

Applications provided by the contractor 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 https://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 contractor may use or incorporate any hardware, software, or services developed or provided by Kaspersky Lab.
No hardware, software, or service provided by the contractor 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 contractor shall incorporate a Supply Chain Risk Management (SCRM) process for any hardware or software provided to the government. The contractor 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/viewhttps://www.fbi.gov/file-repository/scrmbestpractices-1.pdf/view
As determined applicable by the Government, the Contractor agrees to comply with the following statutes, regulations, standards, and policies:
- Federal Information Security Modernization Act, FISMA, of 2014
- Homeland Security Presidential Directive 12 "Policy for a Common Identification

Standard for Federal Employees and contractors”
- The Computer Security Act of 1987
- Office of Management and Budget (OMB) Circular A-130
- 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 Publication 800-53
- National Institute of Standards and Technology, NIST, Special Publication 800-160
- National Institute of Standards and Technology, NIST, Special Publication 800-161
- National Institute of Standards and Technology, NIST, Special Publication 800-171
- Trusted Internet Connections, TIC, initiative (Update), (M-09-32), September 17, 2009
- The Privacy Act

Depending on the types and extent of access to data and systems required for the work, contractor personnel may be required to undergo a background investigation and obtain a security clearance. The contractor 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 Contractor fails to comply with the cybersecurity and privacy requirements, the Contractor shall be deemed to have failed to perform the provision of this contract.
Contractor 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.

Privacy Act notification: If applicable, the Contractor will be required to design, develop, or operate system(s) of records on individuals, to accomplish an Agency function subject to the Privacy Act of 1974, Public Law 93 579 (5 U.S.C., Section 552a) as amended (the Act), and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties Federal Acquisition Regulation, FAR, 52.224 1. The title(s) of the system(s) of records shall be listed on the respective task orders, as appropriate.
The Contractor agrees to:
a. Comply with the Act and the Agency rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
(1) the system(s) of records; and
(2) the design, development, or operation work that the Contractor is to perform.
b. Include the Privacy Act provisions contained in this contract in every solicitation and every subcontract, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act.
c. Include, in all data solicitations requesting information to be placed in a Privacy Act System of Records, a Privacy Act notification statement provided by the DOL.

All Contractor 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 Contractors.
a) Consult with the COR to determine the level of security required for Contractor employees.
b) Ensure the Contractor has all required documents and approvals from the COR.
c) Arrange with the COR for the date, time, and location for Personal Identity Verification, PIV also known as ID, card processing.
d) Ensure that Contractor employees report, with all required documents, to the reporting location determined by the COR.
Upon submission of required PIV documents, Contractor 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 Contractor through the COR. The Contractor shall assume responsibility that these procedures are followed.
Cybersecurity and Privacy Training: (Per Contracting Officer Notice 2018-31) Where required and applicable, contractor employees, including employees of subcontractors 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.

Security Requirements for Application Development

I. GENERAL

The Contractor 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 contractors, subcontractors or other entities hired by Contractor.

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

The Contractor 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 Contractor 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.

Personnel

The Contractor 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.

Security Training

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

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

The Contractor 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.

Background Checks of Developers

The Contractor 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.

Vulnerabilities, Risks and Threats

The Contractor 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 Contractor shall identify the key risks to the important assets and functions provided by the application. The Contractor shall conduct an analysis against an industry recognized list of common programming errors – such as the *SANS Top 25 Most*https://www.sans.org/top25-software-errors/*Dangerous Programming Errors* – current security risk and vulnerabilities – such as *Open Web Application Security Project (OWASP Top Ten)* – and document in writing that they have been mitigated. The Contractor 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 Contractor 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.

Application Development

The Contractor 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 Contractor 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 Contractor 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 contractor 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 Contractor shall specify in writing to the Government what additional industry security standards and level of care that they follow.
The Contractor shall agree in writing to comply with such standards and level of care. The Contractor shall provide written documentation to the Government that clearly explains the design for achieving each of the security requirements. The Contractor 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 Contractor 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 Contractor 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 Contractor shall disclose what tools are used in the software development environment to encourage secure coding.
(b) Configuration Management
The Contractor 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 Contractor 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 Contractor 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 Contractor 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 Contractor 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 Contractor shall implement the security test plan and provide the test results to the Government in writing.
(b) Source Code
The Contractor 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 Contractor shall have a well-documented procedure and framework for conducting code reviews.
The Contractor 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 Contractor shall agree in writing that prior to production the application shall undergo vulnerability and a penetration test.
Post production, the Contractor 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 Contractor shall provide to the Government written documentation of the results of the scans and tests along with a mitigation plan.
The Contractor shall agree in writing that these vulnerabilities shall be mitigated within a pre-negotiated period.
Patches and Updates
The Contractor 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 Contractor shall apply, test, and validate the appropriate patches and updates and/or workarounds on a test version of the application before distribution.
The Contractor shall verify and provide written documentation that all updates have been tested and, prior to production, installed.
The Contractor shall verify application functionality, based upon pre-negotiated procedures, at the conclusion of patch updates, and provide documentation of the results.

Tracking Security Issues
The Contractor 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 Contractor 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 Contractor 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.
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.
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
Acceptance
The software shall not be considered accepted when the Contractor certification package is complete, and all security issues have been resolved.
Investigating Security Issues
After acceptance, if security issues are discovered or reasonably suspected, the Contractor shall assist the Government in performing an investigation to determine the nature of the issue.

1.6.12. Special Qualifications

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 course of 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 2:30 pm Local Time, Monday through Friday, with the exception of Federal Government holidays.

The contractor is responsible for ensuring all employees with development responsibilities shall possess the knowledge and skills necessary to develop and integrate solutions on DOL’s Appian platforms.

1.6.12.1. Business Analyst – (Key Personnel)

Roles and Responsibilities

Lead the technical planning and requirements gathering phases including estimate, develop, test, manage projects, architect, and deliver. Evaluate user requests for business process automation using Appian Business Process Management, BPM, models to determine feasibility and technical requirements. Participate in team design meetings, daily scrum meetings.

Expertise in business process and system analysis, design, improvement, and implementation efforts and in translating business process needs into technical requirements.

- Expertise in change management and training support. Provide organizational and strategic planning for a wide variety of technical and functional environments.
- Expertise in, but not limited to, Configuration Management, Strategic Planning, Knowledge Management, Business Analysis and Technical Analysis.
- Bachelor's degree in Computer Science, Information Systems, Business, or other relevant discipline.
- At least 5 years of current experience or an equivalent combination of technical education and experience.
- Certified Scrum Master.

1.6.12.2. Senior-Level Developer (Key Personnel) Roles and Responsibilities

The senior developer will design and develop the core Appian platform project from end to end. Working closely with Product Owner, and IT Federal Project Manager, FPM, to fully understand the functional and technical requirements in the case management. Actively participate and provide inputs in the major design decisions. Work with Business Analysts, SME's, system owners, customers and end-users to understand their mission, current architecture, security requirements and deliverables. With a focus on the project release goals, work with the team to build a design that will scale to meet the evolving needs. Design and develop the system to set the standard for future development, craft an architecture that smoothly works with existing infrastructure without compromising security. Identify and introduce new opportunities to build platform-based solutions to help the users meet their toughest challenges.

Provide technical leadership to agile development teams, including assigning work and reviewing work products from subordinate developers.

- Present and explain technical material to senior levels of the client organization.
- Design architectural frameworks and solutions using industry-standard methodologies.
- Resolve systems integration issues
- Strong writing, analytical, and presentation skills.
- Certification in Appian Application Designer
- Experience as the technical lead on agile development teams, including assigning work and reviewing the quality of work products from subordinate developers.
- Experience explaining and presenting technical material to senior levels of the client organization.
- At least 7 years of current technical experience or an equivalent combination of technical education and experience.
- At least 5 years of experience designing architectural frameworks using industry-standard methodologies and resolving systems integration issues.
- At least 3 years of experience designing solutions using enterprise business process modeling (BPM) implementation for the Federal Government.
- At least 3 years of experience supporting agile based development teams
- Appian A-Score Certification Level 2 or higher.
- Certification in Appian Application Designer

1.6.13. Post Award Conference/Periodic Progress Meetings:

The Contractor 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 contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor 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.

1.6.14. Contracting Officer Representative (COR):

A COR will be delegated under separate cover. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral

communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract.

1.6.15. Program Manager:

The contractor shall provide a program manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor 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 contractor on all matters relating to daily operation of this contract.

1.6.16. Identification of Contractor Employees:

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor 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 contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

PART 2 DEFINITIONS & ACRONYMS

2.1 Definitions

Best Effort. 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.

PWS. Performance Work Statement

Contracting Officer's Representative (COR). 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.

DOL. Department of Labor

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

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

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

2.2 Acronyms

This section should also contain a complete listing of all acronyms used, giving both the acronyms and the words represented by the acronym. This performance work statement (PWS) contains numerous acronyms. Whenever a new term is introduced in the PWS that shall be referred to by an acronym, the acronym will appear next to the term in parentheses ().

The acronyms that will appear in the PWS are listed below for easy reference:

API - Application Programming Interface
ATO - Authority to Operate
AWS – Amazon Web Service
BAS – Business Application Service
CFO - Chief Financial Officer
CICD - Continuous Integration & Continuous Delivery
CO - Contracting Officer
CONUS - Continental United States
COR - Contracting Officer's Representative
COTS - Commercial Off The Shelf software
DevOps - Development and Operations
DHS - Department of Homeland Security
DOL - Department of Labor
EBSA - Employee Benefits Security Administration
FAR - Federal Acquisition Regulation
FEAF - Federal Enterprise Architecture Framework
FIPS PUB - Federal Information Processing Standards Publication
FOIA - Freedom of Information Act
FPM – Federal Project Manager
GPMS – Grantee Performance Management System
HSPD - Homeland Security Presidential Directive
IT - Information Technology

MSHA - Mine Safety & Health Administration
MSPA - Migrant and Seasonal Agricultural Worker Protection Act
MVP - Minimum Viable Product
NACI - National Agency Check with Inquiries
NSA - National System Administration
O&M - Operations and Maintenance
OCIO - Office, Chief Information Officer
OMB - Office of Management and Budget
OS - Operating System
OSDS - On Site Duty Station
OSHA - Occupational Safety and Health Administration
PII - Personally Identifiable Information
PIV - Personal Identity Verification
PMP - Project Management Plan
PWS - Performance Work Statement
QASP - Quality Assurance Surveillance Plan
QCP - Quality Control Plan
SAFe - Scaled Agile Framework
SDLC - Software Development Lifecycle
SSO – Single Sign On
TAA – Trade Adjustment Assistance
TO - Task Order
TDD - Test Driven Development
UI - User Interface
USC - U.S. Code
WHD - Wage and Hour Division
WHISARD - Wage Hour Investigative Support and Reporting Database
WIOA – Workforce Innovation & Opportunity Act
WIPS – Workforce Integrated Performance System
YB - Youth Build

PART 3 Government Furnished Property, Equipment, and Services

3.1 General:

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

3.2 Equipment:

The Government will provide laptop and necessary software to perform this task order.

If available, the Government will provide working space including furniture, computers, network connections, and telephone access for official work-related calls only. Appropriate software will be provided on-site for use in task completion.

The Contractor shall keep and maintain an inventory of Government-furnished equipment, which shall be made available to the Federal Program Manager upon request.

The Contractor shall be responsible for the Security and Integrity of any Government Furnished Equipment, GFE, and any data it contains used off-site, with prior approval from the Government.

3.3 Services:

3.3.1 Utilities

All utilities in the facility will be available for the contractor's use in performance of duties outlined in this PWS. The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities.

3.4 Facilities:

The Government will furnish the necessary workspace for the contractor staff to provide the support outlined in this PWS to include desk space, telephones, computers and other items necessary to maintain an office environment.

PART 4 CONTRACTOR FURNISHED 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 a [insert clearance level] clearance. The Contractor's employees, performing work in support of this contract shall have been granted a [insert clearance level] security clearance.

PART 5 SPECIFIC TASKS

The Contractor shall continue perform the development tasks of YB-DINAP listed in **Technical Exhibit 3: Schedule and Deliverables** including the following specific tasks.

5.1 Task 1 Phase-In

Phase-In shall commence upon Task Order award, for a total of 30 days. 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 Phase-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/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
- Conduct BA Analysis with the COR, PM, and/or business stakeholders to fully understand and assess the requirements and Use Cases for the current YB-DINAP production system, and the legacy DINAP(SYS) – Youth scope, requirements as well as applicable documentation.
- Report Phase-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 current backlog of YB-DINAP requirements to develop and deploy in upcoming production releases.
- Attend Technical Exchange Meetings (TEMs) with the outgoing Contractor to gain knowledge of the systems and activities, including sustainment

5.2 Task 2. Program and Project Management

The Contractor shall follow guidance from the Federal PM to provide project management support in establishing 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 work closely with the Federal PM to 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 at a DOL Share Point location all system documentation, which includes requirements specifications, user stories, design documentation and test case documentation.
- The Contractor shall provide detailed System design analysis, Architecture overview and Business workflows for the new YB-DINAP system platform features, functional overview, and data architecture.
- legacy The contractor on submission of roadmap, functional requirements specifications and user stories will work in close coordination with other YB-DINAP contractors and SME's if any to validate the requirements to meet the acceptance criteria defined.
- The Contractor shall work in close coordination with other contractors to be part of an agile cadence to enable participate and contribute to Daily Scrums, Backlog Refinement, Sprint Retro, Sprint Review, and other status meetings.

5.3 Task 3. Solutions Architecture and Business Analysis

- The Contractor shall architect and create DOL Agile artifacts for the proposed DINAP (SYS) Youth system solution.
- The proposed solutions shall include a proposed architecture for implementing the Epics, User Stories, Capabilities, Features, and a workflow, as well as database architecture and approach to integrate the DINAP (SYS) Youth application with the YBDINAP database management.
- The Contractor shall lead requirements elicitation discussions with stakeholders, documenting requirements, e.g., creating process flow diagrams, wireframes, use cases, test cases etc.

• The Contractor shall obtain and document requirements by examining pre-existing documentation such as process flow diagrams, use case documents, and other project related documentation.

5.4 Task 4. System Integration and Engineering Services

The Contractor shall conduct the following system integration and engineering services activities:

• As directed by the COR/PM, develop/update and maintain an interface control document (ICD). The ICD shall reflect integration points between YB-DINAP and other DOL OCIO Systems. In addition, the ICD shall include information of the timeline for the integration, the frequency of the data exchange, target-source mapping, budget and acquisitions dependencies, risks and mitigation strategies.

5.5 Task 5. Database Management

• The Contractor shall prepare data call responses as directed by the YB-DINAP COR/FPM. Data calls typically involve aggregating and reporting on application systems attributes such as operating system, server information, programming language, software/hardware, database version, number of releases by calendar year and/or fiscal year, number of active and/or inactive user accounts, etc.
• DOL anticipates a cadence of approximately 1 weekly data migration status meeting and 2 data calls per quarter.
• The Contractor shall ensure that the COR/FPM approved data call is uploaded to DOL YBDINAP 's SharePoint project repository.

5.6 Task 6. Test Plan and Execution

• In addition to testing for each Sprint Cycle and in preparation for the Production Releases, the Contractor shall coordinate and perform the following test activities:
o Unit Testing o System Integration Testing o Performance/Load Testing o 508 Compliance Testing o Regression Testing
o User Acceptance Testing (UAT) – Facilitate and Assist o Develop test scenarios/cases for use during UAT
o Schedule UAT kickoff sessions (up to 3 UATs sessions per release) o Provide user support during UAT
• The Contractor shall provide test scripts and data to conduct sprint reviews and UAT with stakeholders.
• The Contractor shall modify and regression test code to resolve errors found during UAT to ensure the system is ready for production deployment. All changes shall be documented in the DOL OCIO's change control/configuration management tools.
• The Contractor shall document the test results and then upload the results to the project repository (e.g., DOL SharePoint).
Note: Automated testing processes shall be used whenever possible.
Two weeks Agile Sprint Cycles (unless otherwise directed by the FPM)
The Contractor shall conduct bi-weekly sprint reviews that consist of the following:
Presentations (in PowerPoint) and demonstrations (if applicable) of what has been 'done' during the sprint cycle, along with the number of points / velocity. The definition of 'done' will be defined during Sprint 0 and follow-on Sprints by the FPM or Product Owner.
• Lessons learned (i.e., sprint retrospective) from the sprint shall be part of the sprint review presentation.
• Plans for the next sprint cycle per feedback from the PM shall be part of the sprint review presentation.
• Draft versions of (living) documentation (e.g., Design Specification, Requirements, Test Summary Report and Test Results) that have been updated as a result of the sprint shall be delivered prior to the sprint review and noted in the sprint review presentation.
• Plan, implement, and facilitate Sprint User Acceptance Testing (UAT) sessions to allow users to test the functionalities/features of the user stories that were developed during the Sprint cycles**.**

5.7 Task 7. Operations and Maintenance (O&M) and Support Services

Operations and Maintenance (O&M) activities focus on routine support required to maintain the availability, reliability, and security of YB-DINAP. The Contractor shall provide the full range of O&M support services including issue identification, tracking, analysis, and resolution; code generation, testing, COTS customization and configuration; documentation; change incorporation; maintenance of tools, custom code, specialized configurations, customizations and process automation such as scripts, templates, and workflows; performance tuning and monitoring; system administration, and user account administration.

The Contractor shall perform O&M activities in accordance with DOL Agile processes for system development lifecycle activities for the Youth Build / DINAP case management system, such as documentation, software upgrades/patching, API and hosting infrastructure, etc. Youth Build / DINAP project work that is included under this category includes all Youth Build / DINAP system

components and infrastructure.

The contractor shall:

Work collaboratively with users, system administrators, developers, and other stakeholders as needed to resolve system issues, such as system outages, bugs, etc. Bug fixes must be prioritized to support statutory and regulatory timelines.
Document business requirements and implement necessary enhancements to maintain the Youth Build/DINAP Appian system (e.g., updating reference data, modifying templates, user interface changes, storage, reporting, etc.). Reference table updates may be ad hoc or on a scheduled basis.
Document technical requirements and implement necessary enhancements to maintain and improve system functionality. Enhancements include but are not limited to:

- Operate and maintain the Youth Build/DINAP platform in accordance with regulatory requirements. Recommend process improvements, links to additional resources, and uses for the Youth Build/DINAP data streams.
- Immediately following deployments to the production environment, provide postimplementation support (i.e., hyper care or surge) to ensure unforeseen technical or training issues are addressed and resolved.
- Conduct routine system testing to support application-filing load and adequately prepare the system for peak filing periods, should there be a spike in filings.
- Develop and update plans for system support during peak filing times, identifying key infrastructure components, monitoring plans, and recommendations for scaling and capacity changes.
- Conduct table-top and other exercises with technical teams.
- Work collaboratively with the OCIO to address any security vulnerabilities through a variety of methods, such as applying security patches, modifying software code, reconfiguring system settings, etc.
- Follow all established change management procedures to ensure changes introduced to the production environment are thoroughly tested and can be rolled back if needed.
- Develop and maintain System Manual/SOP that includes information to describe the design, development, production, distribution, operation, maintenance and management of the system. Shall include processes and procedures that are required for access, SDLC environment changes, links to applicable tools such as JIRA, GitLab, MS Teams, Service Now, CM knowledge base, SDLC environments, etc.
- Submit Incident Tickets and Change Requests in Service Now for all code changes and code promotions.
- Configure and maintain appropriate system permissions and other system settings.
- Create, update, and maintain system manuals and other system-related documentation in an organized manner and store documentation in official Government document management systems.
- Provide external users and impacted agencies with relevant change management, communications, and training materials to use the system.

5.8 Task 8. Training Support

The Contractor shall provide training support for YB-DINAP in accordance with the Project Process Agreement (PPA) for each release (DME or O&M). The Contractor shall perform the following activities:

- Develop a training plan to include an outline of the training content and timeline/schedule (of releases) for approval by the COR and/or FPM

5.9 Task 9. Transition-Out

Transition Out shall commence 30 days prior to the end of the period of performance. During this time, the Contractor shall provide support services to the orderly transition of functions from this task order 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 Task Order, 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 task order 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 Government-Furnished Information, GFI, e.g., badges and laptops DOL has received all source code and database scripts.

PART 6 APPLICABLE PUBLICATIONS

6.1 Publications Applicable to This PWS: N/A

6.2 DOL Standards, Policies and Procedures

The contractor is responsible for following all relevant DOL Standards, Policies, and Procedures whether they be existing or newly created. Below is a current list of the most relevant standards, policies, and procedures, but this list may change (i.e., add, modify, or delete) over time at the Government's discretion. The contractor is expected to stay informed of these standards, policies, and procedures as they evolve.

- Target Architecture and Strategic Roadmap (TASR)
- DOL Systems Development Life Cycle Manual (SDLCM)
- Program Review Board (PRB)
- Production Release Engagement Process (PREP)
- Enterprise Architecture (EA)
- Capital Planning & Investment Control (CPIC)
- Computer Security Handbook
- Section 508
- DOL Digital Government Strategy
- Mobile Device Management (MDM)

6.3rity Federal Legislation, Policy and Regulatory Guidance:

The contractor must comply with Federal legislation, policy and regulatory guidance, including but not limited to:

- Federal Information Security Modernization Act of 2014 (FISMA)
- Office of Management and Budget (OMB)policy and guidance for privacy and securing federal information and IT systems
- Federal Risk and Authorization Management Program (FedRAMP)
- National Archives and Records Administration (NARA)
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards, FIPS, and Special Publications 800 series

PART 7 TECHNICAL EXHIBIT INDEX

1. Technical Exhibit 1 – Performance Requirements Summary
2. Technical Exhibit 2 – Deliverables Schedule

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 Task Order are all the applicable Business Applications Services (BAS) Performance Requirements listed in the table below.

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.

The IT FPM and COR 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 Contractor will meet with the IT FPM and 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 Contractor will provide a root-case assessment of failures, as well as the status of the corrective action taken.

Types of Surveillance:
Random Sampling: Appropriate for frequently recurring tasks. Evaluate randomly selected samples of the lot to determine the acceptability of the entire lot.
Random Inspection Guide, Method of surveillance, Lot size, Sample size, Performance requirement, Sampling procedure, Inspection procedure
100 Percent Inspection: Appropriate for tasks that occur infrequently. Inspect and evaluate performance each time task is performed
Periodic Surveillance: Evaluation of samples selected on other than 100% or statistically random basis. (I.e. monthly, quarterly, semi-annually etc.)
Validated Customer Complaint: Complaints must be validated.
Please Note: Any surveillance method used in the commercial market to surveil the required service may be used.

TECHNICAL EXHIBIT 1 - Performance Requirements Summary
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 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).

2	Requirements	Build and refine Product Backlog	Maintain 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).
3	Development-Sprint	Sprit 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).
4	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).
5	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).
6	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 Jira data entry. No more than one reminder per quarter.	Jira fields review (Periodic Surveillance).
7	Development-Sprint	Sprint Execution	Deliver agreed-to functionality for the monthly sprint throughout the duration of the project,	Functionality delivered in the sprint reflects discussed and	Completes 95% of tasks according to the	Schedule variance - actual vs

			ensuring required artifacts are produced for each release and the quality of the work is within acceptable standards.	documented acceptance criteria provided by the Government for each approved user story assigned to the current sprint.	project schedule. +/- 5% variability for a release.	baseline (100 Percent Inspection).
8	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).
9	Development-Sprint	Sprint Execution	Execute and document code review for each sprint in addition 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).
10	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 reports (Random Sampling).
11	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).
12	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	Web Content Accessibility Guidelines 2.1 AA standards	Periodic Surveillance

				accordance with departmental guidelines and reflected in each sprint. Use OCIO required tools to test 508 compliances.	much be followed for each sprint. Must pass the core 508 requirements 100%.	
13	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).
14	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).
15	Development-Sprint	Sprint Development	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).
16	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-premises 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).
17	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).
18	Development-Sprint	Coding standards and best practices	Relevant Industry coding standards and best practices are implemented all the time.	At a minimum, general OCIO development guidelines are	There should be no more than 10% of code	Federal architect review

				followed and implemented to ensure code quality (readability, maintainability, reusability & lower technical debt).	quality variation from OCIO defined code development guidelines.	(Periodic Surveillance).
19	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).
20	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).
21	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).
22	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).
23	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).
24	Communications	Contractor Support and Escalation	Maintain and provide to the Government on at least a quarterly basis a support and	Ensure the Government is provided a well-	Government is provided a well-maintained list	Review and approval by the Federal IT

		Contact List	escalation contact list.	maintained support and escalation contact list related to any service components at least on a quarterly basis.	of support and escalation contact list on at least a quarterly basis 100% of the time.	Project Manager (Periodic Surveillance).
25	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).
26	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).
27	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).
28	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).
29	Secure Software Attestation	Attestation	Complete Secure Software Development standard attestation with each delivery.	Ensure development standards are complied with.	100%	Review and approval by the Federal IT Project Manager (100 Percent Inspection).

TECHNICAL EXHIBIT 2

Deliverables Schedule

Task	Deliverable	Due	Format	Submit To
Transition-In PWS 5.1	Contractor personnel suitability (e.g., background investigation) packages	14 calendar days from award	Resume, PIC, OF-306, and eQIP	COR
Transition In, PWS 5.1	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)	By 10th of each Month	Word or PowerPoint	COR and Federal Project Manager
All	Monthly invoices	Monthly by the 10th of the month	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	Federal Project Manager

			performance metrics	
DME	Updated Product Backlog	1 calendar days after Sprint start	Jira	Jira
Transition-Out, PWS 5.9	Transition plan	60 calendar days before project end	Word/PDF	COR and Federal Project Manager
Transition-Out, PWS 5.9	Finalized implementation and support documents	30 calendar days before project end	Source/PDF	COR and Federal Project Manage
Transition-Out, PWS 5.9	Source code, configurations, etc.	30 calendar days before project end	Gitlab	COR and Federal Project Manager
Transition-Out, PWS 5.9	List of government provided GFE returned and accepted	Upon project end	Word/Excel	COR and Federal Project Manager

D - Contract Clauses

Clause List

52.217-8 Option To Extend Services. (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 days.

(End of clause)

52.217-9 Option To Extend the Term of the Contract. (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 5 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 5 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 48 months.

(End of clause)

52.237-3 Continuity of Services. (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to (1) furnish phase-in training and (2) exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (*i.e.*, costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

(End of clause)

PART 2952 SOLICITATION PROVISIONS AND CONTRACT CLAUSES

2952.201-70 Contracting Officer's Representative (COR) Clause. (SEP 2014)

(a) A Contracting Officer's Representative (COR) will be delegated upon award. A copy of the delegation memorandum will be provided to the COR and a delegation letter sent to the vendor.

(b) The COR is responsible as applicable for receiving all deliverables; inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor which

clarifies the contract effort, fills in details or otherwise serves to accomplish the contractual scope of work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If, as a result of technical discussions, it is desirable to alter/change contractual obligations or the scope of work, the contracting officer must issue such changes.

(End of Clause)

2952.204-70 Records Management Requirements. (AUG 2018)

A. Definitions

"Federal record," as defined in 44 U.S.C. 3301, includes all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term federal record:

(a) Includes DOL records.

(b) Does not include personal materials.

(c) Applies to records created, received, or maintained by contractors pursuant to their DOL contract.

(d) May include deliverables and documentation associated with deliverables.

B. Requirements

(a) Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to, the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR chapter XII, subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

(b) In accordance with 36 CFR 1222.32(b), all data created for Government use and delivered to, or falling under the legal control of, the Government are federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

(c) In accordance with 36 CFR 1222.32, contractor shall maintain all records created for government use or created in the course of performing the contract and/or delivered to, or under the legal control of, the Government and must be managed in accordance with federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(d) DOL and its contractors prevent the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of DOL or destroyed except for in accordance with the provisions of the applicable agency schedules and with the written concurrence of the Head of the Contracting Activity in consultation with the Agency Records Officer. Willful and unlawful destruction, removal, damage, or alienation of federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, the contractor must report the event to DOL. The agency must report the incident directly to their Agency Records Officer. The Agency Records Officer will engage the Departmental Records Officer who will follow procedures promptly to report to NARA in accordance with 36 CFR part 1230.

(e) The contractor shall immediately notify the appropriate contracting officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and

confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The contractor shall not remove material from government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records, and/or equipment is no longer required, it shall be returned to DOL's control, or the contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the contracting officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with paragraph (d) of this clause.

(f) The contractor is required to obtain the contracting officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material, and/or records generated under, or relating to, contracts. The contractor (and any sub-contractor) is required to abide by government and DOL guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

(g) The contractor shall only use government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with DOL policy.

(h) The contractor shall not create or maintain any records containing any non-public DOL information that are not specifically tied to or authorized by the contract.

(i) The contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

(j) [[Insert the following if no other data rights clause has been included in the contract]] The DOL owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which DOL shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through 52.227-20.

(k) Training. All contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take the annual mandatory records management training, provided by DOL, as directed by the Contracting Officer's Representative (COR). The training shall be completed in a timeframe specified by the COR. The contractor confirms training has been completed according to agency policies, including initial training and any annual or refresher training.

C. Flow Down of Requirements to Subcontractors

(a) The contractor shall incorporate the substance of this clause, its terms, and requirements, including this paragraph, in all subcontracts under this contract and require written subcontractor acknowledgment of same.

(b) Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

(End of Clause)

2952.207-70 Contractor Personnel Telework. (OCT 2021)

The Government shall not provide or reimburse contractor personnel for internet connectivity.

(End of Clause)

2952.209-70 Organizational Conflict of Interest Clause-OCI-1 Exclusion From Future Agency Contracts. (DEC 2012)

This clause supplements the FAR provisions on organizational conflicts of interest, located at FAR subpart 9.5 and should be read in conjunction with these provisions. To the extent there is any inconsistency or confusion between the two provisions, the FAR provision controls.

(a) Work under this contract may create a future organizational conflict of interest (OCI) that could prohibit the contractor from competing for, or being awarded, future government contracts. The following examples illustrate situations in which

organizational conflicts of interest may arise. They are not all inclusive, but will be used by the contracting officer as general guidance in individual contract situations:

(1) Unequal Access to Information. The performance of this contract may provide access to "nonpublic information," which could provide the contractor an unfair competitive advantage in later solicitations or competitions for other DOL contracts. Such an advantage could be perceived as unfair by a competing vendor who is not given similar access to the same nonpublic information that is related to the future procurement action. If you, as a contractor, in performing this contract, obtain nonpublic information that is relevant to a future procurement action, you may be required to submit and negotiate an acceptable mitigation plan prior to being deemed eligible to compete on the future action. Alternatively, the "nonpublic information" may be provided to all offerors.

(2) Biased Ground Rules. Your contract with DOL may have, in some fashion, established important "ground rules" for another DOL procurement, in which you may desire to be a competitor. For example, this contract may involve you drafting the statement of work, specifications, or evaluation criteria for a future DOL procurement. The primary concern, in any such situation, is that any such firm could skew the competition, whether intentionally or not, or be perceived as having skewed the competition, in its own favor. If the requirements of this DOL contract anticipate the contractor may be placed in a position to establish important ground rules, including but not limited to those described herein, the contractor may be precluded from competing in the related action or, if possible, may be required to submit and negotiate an acceptable mitigation plan.

(3) Impaired Objectivity. The performance of this contract may result in the contractor being placed in a situation where it is able, or required, to provide assessment and evaluation findings concerning itself, another business division, a subsidiary or affiliate, or other entity with which it has a significant financial relationship. The concern in this case is that the contractor's ability to render impartial advice to DOL could appear to be undermined by the contractor's financial or other business relationship to the entity whose work product is being assessed or evaluated. In these situations, a "walling off" of lines of communication between entities or divisions may be acceptable, but it also may not be sufficient to remove the perception that the objectivity of the contractor has been tainted. If the requirements of the DOL procurement indicate that a contractor may be placed in a position to provide evaluations and assessments of itself or other entities with which it has a significant financial relationship, the affected contractor should notify DOL immediately. The contractor may also be required to provide a mitigation plan that includes recusal by the contractor from one of the affected contracts. Such recusal might include divestiture of the work to a third party.

(b) To prevent a future OCI of any kind, the contractor shall be subject to the following restrictions:

(1) The contractor may be excluded from competition for, or award of, any government contracts as to which, in the course of performing another contract, the contractor has received nonpublic and competitively relevant information before such information has been made generally available to other persons or firms.

(2) The contractor may be excluded from competition for, or award of, any government contract for which the contractor actually assisted or participated in the development of specifications or statements of work.

(3) The contractor may be excluded from competition for, or award of, any government contract which calls for it to evaluate itself, any affiliate, or any products or services produced or performed thereby.

(4) The contractor may be excluded from competition for, or award of, any government contract calling for the production or performance of any product or service for which the contractor participated in the development of requirements or definitions pursuant to another contract.

(c) This clause shall not exclude the contractor from performing work under any modification to this contract or from competing for award of any future contract for work that is the same or similar to work performed under this contract, so long as the conditions above are not present. This clause does not prohibit an incumbent from competing on a follow-on competition, but the contracting officer may require a mitigation plan or other steps as needed to ensure that there has not been an unequal access to nonpublic competitively sensitive information.

(d) The term "contractor" as used in this clause, includes any person, firm, or corporation that owns or controls, or is owned or controlled by, the contractor. The term also includes the corporate officers of the contractor.

(e) The agency may, in its sole discretion, waive any provisions of this clause if deemed in the best interest of the Government. The exclusions contained in this clause shall apply for the duration of this contract and for three (3) years after completion and acceptance of all work performed hereunder, or such other period as the contracting officer shall direct.

(f) If any provision of this clause excludes the contractor from competition for, or award of any contract, the contractor shall not be permitted to serve as a subcontractor, at any tier, on such contract. This clause shall be incorporated into any subcontracts or consultant agreements awarded under this contract unless the contracting officer determines otherwise.

(End of Clause)

2952.211-70 Internet Protocol Version 6 (IPv6) Clause. (MAY 2015)

(a) Any system or product that includes: hardware, software, firmware, and/or networked components, including but not limited to, voice, video, or data that is developed, procured, or acquired in support and/or performance of this requirement shall be capable of transmitting, receiving, processing, or forwarding digital information across system boundaries that are formatted in accordance with commercial standards of Internet Protocol (IP) version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program.

(b) This IPv6 capable system or product shall maintain interoperability with IPv4 systems and provide the same level of performance and reliability capabilities of IPv4 systems.

(c) This IPv6 capable system or product shall have available IPv4 and IPv6 technical support for development, implementation, and troubleshooting of the system.

(d) This IPv6 capable system or product can be upgraded, or the vendor will provide an appropriate migration path for industry-required changes to IPv6 as the technology evolves, at no additional cost to the Government.

(e) This IPv6 capable system or product must be able to operate on networks supporting IPv4 & IPv6, as well as networks that support both.

(f) Any system or product whose IPv6 non-compliance is discovered and made known to the vendor/contractor within 12 months of the start of performance shall be upgraded, modified, replaced, or brought into compliance at no additional cost to the Federal Government.

(End of Clause)

2952.224-70 Privacy Breach Notification Requirements. (APR 2018)

A. Definitions

"Breach" is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where-

(a) A person other than an authorized user accesses or potentially accesses Personally Identifiable Information (PII); or

(b) An authorized user accesses or potentially accesses PII for an unauthorized purpose.

"Information" is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).

"Information System" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

"Personally Identifiable Information" is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual (see OMB Circular No. A-130, Managing Federal Information as a Strategic Resource).

B. Requirements

(a) Contractors and subcontractors that collects or maintains federal information on behalf of the agency or uses or operates an information system on behalf of the agency shall comply with federal law *e.g.*, FISMA 2014, E-Government Act and the Privacy Act. Additionally, the contractor shall meet OMB directives and National Institute of Standards and Technology Standards to ensure processing of PII is adequately managed.

(b) The contractor shall:

(1) Properly encrypt PII in accordance with appropriate laws, regulations, directives, standards, or guidelines;

(2) Report to DOL any suspected or confirmed breach in any medium or form, including paper, oral, and electronic within one hour of discovery;

(3) Cooperate with and exchange information with DOL (contracting officer and Contracting Officer's Representative) as well as allow for an inspection, investigation, forensic analysis, as determined necessary by the DOL, to effectively report and manage a suspected or confirmed breach;

(4) Maintain capabilities to determine what DOL information was or could have been compromised and by whom, construct a timeline of user activity, determine methods and techniques used to access federal information, and identify the initial attack vector;

(5) Ensure staff who have access to DOL systems or information are regularly trained to identify and report a security incident. This includes the completion of any DOL mandatory training for contractors;

(6) Take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised.

(7) Report incidents per DOL incident management policy and US-CERT notification guidelines.

(c) Remedy:

(1) A report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII. If the contractor is determined to be at fault for the breach, the contractor may be financially liable for government costs incurred in the course of breach response and mitigation efforts;

(2) The contractor shall take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised. Additionally, the individual or individuals directly responsible for the data breach shall be removed from the contract within 45 days of the breach of data; and

(3) The Government reserves the right to exercise all available contract remedies including, but not limited to, a stop-work order on a temporary or permanent basis to address a breach or upon discovery of a contractor's failure to report a breach as required by this clause. If the contractor is determined to be at fault for a breach, the contractor shall provide credit monitoring and privacy protection services for one year to any individual whose private information was accessed or disclosed. The individual shall be given the option, but the decision is theirs. Those services will be provided solely at the expense of the contractor and will not be reimbursed by the Federal Government.

(End of Clause)

2952.232-70 Limitation of Government's Obligation (LoGO). (JUL 2014)

(a) Contract line item(s) ($ to be determined at the exercise of each option) through ($ to be determined at the exercise of each option) are incrementally funded. For these item(s), the sum of ($ to be determined at the exercise of each option) of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the

Government's convenience, approximates the total amount currently allotted to the contract. The contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the contractor will notify the contracting officer in writing at least thirty days prior to the date when, in the contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 80 percent of the total amount presently allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the contracting officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the contractor's notification, or by an agreed substitute date, the contracting officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance, which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes." In no event shall the equitable adjustment be more than the contract line item(s) price(s) in question.

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract $[___]*

[(month)] [(day)], [(year)] $[___]*

[(month)] [(day)], [(year)] $[___]*

[(month)] [(day)], [(year)] $[___]*

* To be inserted after negotiation.

(End of Clause)

2952.232-71 Submission of Invoices. (AUG 2019)

(a) Electronic Invoice Submittal Invoices for the services/goods provided under this award shall be submitted through the Department of Treasury's Invoice Processing Platform (IPP) or through the DOL Quickpay email system, as directed by the Contracting Officer. IPP is a Federal Government owned and operated website accessible to contractors free of charge. Information about IPP, including enrollment instructions, are available and should be obtained by the enrolled contractors directly from the Department of Treasury after award at *https://www.ipp.gov*.

(1) The following instructions apply to Invoices submitted through *IPP.Gov* or the DOL Quickpay email system:

(i) IPP invoice attachments SHALL NOT exceed the size limit of 10 megabytes (MB) each. However, you may submit multiple attachments of less than 10MB each with the invoices.

(ii) DO NOT submit an invoice or attachment that uses shading or color.

(b) An emailed Portable Document Format (PDF) image cannot have any text that has a background with any color other than white. If the image has a shaded background, it will be converted to black, and the text will be illegible.

(c) An emailed Tagged Image File Format (TIFF) image must be black and white.

(1) Quickpay users SHALL provide a copy of the invoice and any attachments via email to the Contracting Officer's Representative (COR, at the address specified in the contract.

(2) Quickpay users SHALL NOT submit more than one attachment per invoice and the attachment shall not exceed 10MB. Any additional attachments will not be recognized.

(3) DO NOT submit more than one invoice at a time.

(4) DO NOT attempt to use the "Recall" or "Resend" email message features.

(d) Electronic invoices shall be in PDF or TIFF format.

(e) Paper Invoices shall be submitted via fax or U.S. mail Paper invoices may be sent via fax to: (202) 693-2862. Mail paper invoices to: U.S. Department of Labor, Office of Financial Management Operations Division of Client Accounting, Services Room S-5526, 200 Constitution Avenue NW, Washington, DC 20210.

(f) General Information.

Payment due date is to be calculated from the date the invoice is received in accordance with FAR 32.905 and the instructions above.

Inquiries regarding invoices must be emailed to *OCFOinvoiceinquiries@dol.gov*. The relevant invoice must be attached to the inquiry email and the subject line of the email must state "INQUIRY", as shown in the following example:

INQUIRY: Contractor Name, DOL Agency, Contract Number, BPA Call or Order Number, Invoice Number, Invoice Amount

The contractor SHALL NOT use the DOL electronic invoicing email address for inquiries about any invoice.

Questions:

All questions regarding Electronic Invoicing shall be sent to the DOL Office of the Chief Financial Officer (OCFO) at *OCFOinvoiceinquiries@dol.gov*.

(End of Clause)

2952.237-70 Emergency Continuation of Essential Services. (MAR 2014)

(a) Essential Services. DOL has identified certain services under this agreement (contract, BPA, BOA, task/delivery order, or other vehicle, hereinafter "requirement") as being essential to the DOL's missions and operations. Such essential services must continue to be performed, even if an event occurs (or is threatened to occur) that would disrupt or interfere with operations at, or with access to, facilities where services ordinarily take place. Such an event may include, but is not limited to, emergencies that may be natural (*e.g.*, earthquake; flood; hurricane; tornado; public health emergencies, including pandemic influenza), man-made (*e.g.*, civil unrest, chemical spill, cyber or terrorist threats or attacks), or technological (*e.g.*, building fire, utility outage), and which may affect one or more facilities or locations, including federal facilities, where the contractor normally performs services hereunder.

(b) Contingency Plans. Unless already included in the requirement, within 30 days of the commencement of performance (or the bi-lateral incorporation of this clause), the contractor shall submit the following contingency plans to the contracting officer (CO) and the Contracting Officer's Representative (COR):

(1) A contingency plan to continue performance off-site for a period of between 1 and 30 days; and

(2) A contingency plan to continue performance off-site for more than 30 days, until the event described above is resolved.

(3) Such contingency plans will become an obligation of the contractor under the requirement.

(c) Contents of the Contingency Plans. The contingency plans referenced in paragraph above shall, at a minimum, address:

(1) How the contractor plans to continue performance of essential services for the duration of an event, including identifying and securing suitable off-site workplaces, personnel, and resources;

(2) The contractor's use of off-site facilities, including allowing its essential personnel to work from an alternative site or other remote locations to perform essential services;

(3) Alert and notification procedures for mobilizing and communicating with DOL and with essential personnel, and for communicating expectations to its personnel regarding their roles and responsibilities during the event;

(4) A list of telephone numbers and email addresses (with alternates if available) for all managers currently performing under the requirement; and

(5) Processes and requirements for the identification, training, and preparedness of essential personnel who would be capable of relocating to alternate facilities or performing work from home.

(d) Approval of the Contingency Plans. The CO, in consultation as appropriate with the COR, shall review both contingency plans within 14 days of receipt, or as agreed, and shall either accept them or advise the contractor of any reason for disapproval. If either plan is not accepted by the CO, the contractor shall resubmit a revised plan within 7 days, or as agreed.

(e) Activation of a Contingency Plan. The Agency Head, CO, COR, or other authorized agency official may activate the contractor's Contingency Plan by notifying the contractor either orally or in writing. In the event of an oral instruction, a written confirmation of the activation will follow shortly after the resumption of normal activities. Once a contingency plan has been activated, services hereunder shall continue without delay or interruption, notwithstanding the "Excusable Delay" Clause, or any other provision of the contract (or requirement if this contract vehicle is BPA, BOA, or similar vehicle).

(f) Failure to Execute a Plan. In the event the contractor is unable or unwilling to perform the essential services identified under the requirement, as determined by DOL in its sole discretion, DOL reserves the right, in addition to any other right it may have, to use federal employees or other contract support, either from existing contracts or new contracts, to continue those critical services. DOL may view the contractor's failure to implement the Contingency Plan as not performing a contractual requirement and reserves all rights to seek remedies associated with any such nonperformance. Any new contracting efforts would be conducted in accordance with the FAR, OFPP's January 14, 2011 Emergency Acquisition Guide, or any other subsequent emergency guidance that may be issued.

(End of Clause)

2952.239-70 Section 508 Requirements. (AUG 2024)

A. Definition

The term "Information and Communication Technology (ICT)" in this contract is used as defined at FAR 2.101.

B. Requirements

Section 508 of the Rehabilitation Act, as amended (29 U.S.C. 794d), applies to federal departments, such as DOL, and the contractors providing support on behalf of such federal departments. The contractor is required to provide Section 508 compliant systems and components of ICT when federal agencies develop, procure, maintain, or use ICT. The contractor shall ensure that its system and components allow federal employees and members of the public with disabilities access to, and use of, information and data that is comparable to the access afforded federal employees and members of the public without disabilities. Products, platforms, and services delivered as part of this contract action that are ICT, or contain ICT, shall conform to the Revised Section 508 Standards, which are located at 36 CFR part 1194, appendices A and C. Please insert the clause(s) below which meet the parameters of the contract being awarded.

(a) Requirements by service/contract type are as follows:

(1) *Custom ICT Development Services*: When the contractor provides custom ICT development services and/or Commercially Available Off-the-Shelf (COTS) products, pursuant to the requirements, the contractor shall ensure the ICT fully conforms to the Revised 508 Standards (36 CFR part 1194, appendices A and C) prior to delivery and before final Acceptance.

(2) *Installation, Configuration, & Integration Services*: When the contractor provides installation, configuration, or integration services for equipment or software pursuant to the requirement, the contractor shall not install, configure, or integrate the equipment or software in a way that reduces the level of conformance with the Revised 508 Standards (36 CFR part 1194, appendices A and C).

(3) *Maintenance Upgrades & Replacements*: The contractor shall ensure maintenance upgrades, substitutions, and replacements to equipment and software pursuant to this award do not reduce the approved level of conformance with the Revised 508 Standards (36 CFR part 1194, appendices A and C) at the time of award. Additionally, an updated Accessibility Conformance Report (ACR) shall be submitted for the ICT, and the ACR shall be completed according to the instructions provided by the Information Technology Industry Council (ITI) to be considered for each option year exercised.

(4) *Contractor Processes*: The contractor shall ensure that its processes are at a maturity level at least equivalent to the DHS Trusted Tester methodology; that its personnel have the knowledge, skills, and ability necessary to make ICT under this contract conform to the Revised 508 Standards (36 CFR part 1194, appendices A and C); and that it provides conformant Section 508 supporting documentation upon request.

(5) *Hosting Services*: The contractor shall not implement hosting services in a manner that reduces the existing level of conformance of the electronic content with the Revised 508 Standards (36 CFR part 1194, appendices A and C), when providing hosting services for electronic content to the agency. Throughout the life of the award, the agency reserves the right to perform Independent third-party testing on a vendor or contractor's hosted solution to verify conformance.

(b) *Validation for ICT*: The contractor shall test and validate the ICT for conformance to the Revised 508 Standards (36 CFR part 1194, appendices A and C), in accordance with the required testing methods and provide test results to verify conformance of the Voluntary Product Assessment Template (VPAT).

(1) For web and software, WCAG 2.0 Level A and AA Conformance test results shall be based on the Accessibility Tests for Software and Web, Harmonized Testing Process for Section 508 Compliance from the DHS Trusted Tester program.

(2) For Microsoft Office and PDF documents, WCAG 2.0 Level A, and AA Conformance test results shall be based on the Harmonized Testing Guidance from the Accessible Electronic Documents Community of Practice.

(3) For ICT that are not electronic content, the contractor shall validate conformance to the Revised 508 Standards (36 CFR part 1194, appendices A and C) using a defined testing process. The contractor shall describe the test process and provide the testing results to the agency.

(c) *Conformance Reporting*: For ICT that are developed, updated, or configured for the agency, and when product substitutions are offered:

(1) Before Acceptance, the contractor shall provide an Accessibility Conformance Report (ACR) for the ICT that is developed, updated, configured for the agency, and when product substitutions are offered. The ACR should be based on the most recent version of the Voluntary Product Assessment Template (VPAT) provided by the Information Technology Industry Council (ITI). An ACR shall be submitted for each ICT and shall be completed according to the instructions provided by ITI to be considered for Acceptance.

(2) Before Acceptance, when the contractor is required to perform testing to validate conformance to the agency's accessibility requirements, the vendor shall provide a supplemental accessibility report that contains the following information:

i Accessibility test results based on the required test methods.

ii Documentation of features provided to help achieve accessibility and usability for people with disabilities.

iii Documentation of core functions that cannot be accessed by persons with disabilities.

iv Documentation on how to configure and install the ICT to support accessibility.

v. When ICT is an authoring tool that generates content (including documents, reports, training, videos, multimedia productions, web content, etc.), provide information on how the ICT enables the creation of accessible electronic content that conforms to the Revised 508 Standards (36 CFR part 1194, appendices A and C), including the range of accessible user interface elements the tool can create.

vi. Before final Acceptance, the contractor shall provide a fully working demonstration of the completed ICT to demonstrate conformance to the agency's accessibility requirements. The demonstration shall expose where such conformance is and is not achieved.

(3) At any time, DOL reserves the right to perform Independent third-party testing to validate the ICT provided by the contractor, conforms to the Revised 508 Standards (36 CFR part 1194, appendices A and C).

(d) *Non-Compliance*: Before final Acceptance of ICT, including updates and replacements, DOL shall determine that the furnished ICT is in compliance with the Revised 508 Standards (36 CFR part 1194, appendices A and C). If the furnished ICT is determined to be non-compliant, the contracting officer shall notify the contractor of this determination, within 15 business days of determination of non-compliance. The contractor shall, at no cost to DOL, repair or replace the non-compliant products or services within the period specified by the contracting officer. The contracting officer makes the final decision to accept or not accept a contractor's ICT that does not meet the Revised 508 Standards (36 CFR part 1194, appendices A and C).

(End of Clause)

2952.242-70 Access to Contractor Business Systems. (APR 2019)

The contractor shall, upon request, provide to the Government, access to covered contractor systems associated with the execution and performance of this requirement to meet audits, reviews, security requirements, and Office of Inspector General requests.

(End of Clause)

2952.242-71 DOL Mandatory Training Requirements for Contractor Employees. (AUG 2018)

(a) Where required and applicable, contractor employees, including employees of subcontractors 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.

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

(c) The contractor shall ensure this clause is incorporated in all subcontracts, at any tier.

(End of Clause)

2952.243-70 Contractor's Obligation To Notify the Contracting Officer of a Request to Change the Contract Scope (Contractor's Obligation Clause). (JAN 2012)

(a) Except for changes identified in writing and signed by the contracting officer, the contractor is required to notify, within 5 working days of receipt or knowledge, any request for changes to this contract (including actions, inactions, and written or oral communications) that the contractor regards as exceeding the scope of the contract. On the basis of the most accurate information available to the contractor, the notice shall state:

(1) The date, nature, and circumstances of the conduct regarded as a change in scope;

(2) The name, function, and activity of each Government employee and contractor official or employee involved in, or knowledgeable about, such conduct; and

(3) The identification of any documents and substance of any oral communication involved in such conduct.

(b) Following submission of this notice, the contractor shall continue performance in accordance with the contract terms and conditions, unless notified otherwise by the contracting officer.

(c) The contracting officer shall promptly, within 5 business days after receipt of notice from the contractor, respond to the notice in writing. In responding, the contracting officer shall either:

(1) Confirm that the contractor's notice identifies a change in the scope of the contract and directs the contractor to stop work, completely or in part, in accordance with the Stop Work provisions of the contract;

(2) Deny that the contractor's notice identifies a change in scope and instruct the contractor to continue performance under the contract; or

(3) In the event the contractor's notice does not provide sufficient information to make a decision, advise the contractor what additional information is required, and establish the date by which it should be furnished and the date thereafter by which the Government will respond.

(End of Clause)

2952.245-70 Contractor Responsibility to Report Theft of Government Property. (FEB 2020)

Upon the contractor becoming aware of theft of government property by its employee(s), including theft that occurs at subcontractor or alternate site locations, the contractor shall report the theft of government property to the Contracting Officer's Representative or CO of record.

(End of Clause)

2952.245-71 Asset Reporting Requirements. (JUL 2019)

(A) Definitions

"Accountable Property" is a term to identify property that is essential to DOL operations for which it is in the best interest of the Government to assign and record accountability to assure proper use, maintenance, and disposal. This includes items purchased and obtained through a "lease-to-own" program. The following items are DOL Accountable Property:

(1) DOL-owned or DOL-leased serialized items (*i.e.*, items with a manufacturer's serial number) with an acquisition unit cost above $3,000.

(2) DOL-owned or DOL-leased "sensitive items."

(3) DOL-owned or DOL-leased furniture with an acquisition unit cost above $10,000. Items with an acquisition unit cost less than $10,000 are not applicable. "Sensitive Items" are defined as items, regardless of value, that have appeal to others and

may therefore be subject to theft or to security concerns, or that are considered mission critical. The following are considered sensitive items, as well as any other items identified as sensitive by the Contracting Officer's Representative (COR):

(1) Desktops and Laptops, including docking stations and connectable monitors.

(2) PDAs/iPads/SurfacePros/Tablets.

(3) Printers and Copiers.

(4) Software Licenses, including media.

(5) Mobile Devices.

(6) Firearms.

(7) Communication Equipment (*e.g.* telephone base and handsets, mobile radio equipment, etc.).

(8) Conference/Audio-Visual Equipment.

(9) Power/Specialty Tools (*e.g.* lab equipment, postage meters, etc.).

(B) Requirements

The contractor shall submit a DOL Asset Report at time of delivery for both Accountable Property and Sensitive Items. The DOL Asset Report shall be delivered electronically to the COR. DOL Asset Reports shall include Accountable Property and Sensitive Items that have been delivered. The report shall be formatted as an Office Open XML Spreadsheet (.XLSX) document, and adhere to following DOL Asset Report Requirements:

(a) Award/Purchase Number. The award number issued by the Government.

(b) Date Shipped. The date the item was shipped to the Government.

(c) Asset Type. The contract Line-Item Description.

(d) Manufacturer. The manufacturer of the item.

(e) Model. The model (name and/or number) of the item.

(f) Serial Number. The serial number of the item.

(g) DOL Asset Number. The number of the barcode applied before shipping (if barcoding is required by the award).

(h) Government Shipping Street Address. The shipping street address of where the item was delivered.

(i) Warrantied Item. Indicates whether an item is warrantied (Y or N).

(j) Warranty Time frame. The start and end date of the warranty (if applicable).

(k) Cost. Acquisition cost per unit and total cost of purchase.

(End of Clause)

E - Instructions,Conditions, and Notices to Bidders

INSTRUCTIONS, CONDITIONS AND NOTICES TO BIDDERS

The Following instruction to offerors is also applicable to this RFQ and are incorporated herein by reference:

1. North American Industry Classification System (NAICS) code and small business size standard. The NAICS code is 541512.

2. Period of acceptance of offers. The Offeror agrees to hold the prices offer for a Validity Period of 30 days from quote due date, unless another time period is specified in an amendment to the solicitation.

3. Discount terms: The Government encourages the best-discounted price be provided.

4. Pricing: The quote submitted must show an itemized breakdown on the cost for products and/or support services for length of award. Pricing will be evaluated for price reasonableness, including confirmation that the pricing is consistent with the vendor's commercial pricing.

5. Late submissions, modification, revisions, and withdrawals of offers. Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, to the Government by the time specified in block 10 of the SF 18.

6. The prospective awardee shall be registered in SAM database (http://www.sam.gov) prior to award, during performance and through final payment of any contract resulting from this solicitation.

7. Applicable solicitation provisions and contract clauses are provided and are either incorporated by reference (IBR) or in full text.

8. The quote must be received no later than 4:00 PM Eastern Time on Thursday, July 3, 2025, or sooner. The quote shall be submitted via email to: chambers.marlon.k@dol.gov and courtesy copy duncan.jermaine.l@dol.gov. Please reference RFQ 1605TA-25-Q-00039 in the subject line.

EVALUATION CRITERIA AND FACTOR IMPORTANCE
The Government intends to award a contract resulting from this RFQ to the responsible Offeror whose quote represents the Best Value utilizing a "Lowest Price Technically Acceptable" (LPTA) evaluation method. Therefore, each quote will be evaluated for Technical Acceptability and Price.

TECHNICAL ACCEPTABILITY
The Government will evaluate the soundness, completeness, and adequacy of the offeror's discussion of the requirements outlined in the PWS. The contractor shall submit a technical volume outlining the contractor's technical approach to successfully meet the requirements of the PWS.

Standard: The minimum requirement is met only when the offeror adequately demonstrates their technical approach shows an understanding of the PWS requirements.

PRICE
This volume contains all pricing data required by the solicitation. The Contractor shall use the provided Pricing Sheet in section B of this solicitation to submit their pricing and if additional pricing information is required, the Contractor shall include separate pricing documentation. Pricing will be evaluated for price fair and reasonableness.

BASIS OF AWARD
The Government intends to award a Labor-Hour task order resulting from this RFQ to the responsible Offeror whose quote represents the Best Value utilizing a "Lowest Price Technically Acceptable" (LPTA) evaluation method. Therefore, Technical Acceptability and Price shall be the only evaluation Factors.

(END OF SECTION E)

END OF SOLICITATION