Federal Bureau of Prisons
Central Office, Washington, D.C.
Cognitive Assessment
Statement of Work (SOW)

MISSION

This Statement of Work (SOW) outlines the requirements for administering a fully digital comprehensive assessment system designed for the evaluation of cognitive abilities, academic achievement, and oral language skills. The assessment will replace physical test kits with a laptop or tablet configuration.

Additionally, an outline of a multi-model professional development (PD) for Federal Bureau of Prisons (FBOP) Special Education Teachers on the requirements for the administration, scoring, and interpretation of the assessment system. This will include how the assessment, the facilitation of the assessment, and specific training meet the needs and goals of the FBOP.

This document will serve as a guideline for procuring and deploying the necessary technology infrastructure and tools to support these educational objectives.

BACKGROUND

The FBOP is an agency of the Department of Justice (DOJ). It consists of 122 institutions throughout the United States, including Hawaii and Puerto Rico, six regional offices, a Central Office (headquarters), two staff training centers, and 26 Residential Reentry Management offices.

The FBOP is responsible for the custody and care of over 150,000 adult Federal offenders. Approximately 91 percent are confined in FBOP-operated facilities, while the balance are confined in secure privately managed or community-based facilities and local jails.

The FBOP is committed to providing resources to establish a supportive environment promoting the successful reintegration of inmates into the community after completing their sentences.

Federal Bureau of Prisons Reentry Services Division (RSD)/Education Branch is to provide mandatory literacy programs, as required by Federal laws and rules language, which meet the needs and interests of the inmate population, provide options for the positive use of their time, and enhance successful reintegration into the community. In an effort to comply with federal mandate 28 CFR § 544.70, which states that an inmate confined in a federal institution who does not have a verified GED credential or high school equivalent (HSE) diploma is required to attend an adult literacy program for minimum of 240 instructional hours or until a GED is achieved, whichever occurs first and § 523.20(b)(c) which states all yearly awards of good conduct time (GTC) will vest for inmates who have earned, or are making satisfactory progress toward earning a GED credential. The FBOP will provide educational services which potentially lead to a nationally and internationally recognized HSE credential for all Federal prisoners who participate in the literacy program.

All FBOP institutions offer literacy classes, English-as-a-Second Language (ESL), adult continuing education (ACE), career technical education (CTE), library services, and recreation/leisure-time activities (such as structured an unstructured fitness, games, music, and hobby craft) and programs.
In most cases, inmates who do not have a high school diploma or HSE certificate must participate in the literacy program for a minimum of 240 hours or until they obtain the diploma. Non-English-speaking inmates must take English as a Second Language courses.
Each FBOP facility has a recreation health awareness library and a leisure reading library. Educators at each site purchase copies of fiction and nonfiction books, magazines, newspapers, and reference materials. Education staff also work with local libraries to facilitate interlibrary loans of materials not available onsite.

The FBOP provides psychological programing to inmates in the areas of behavioral management, rehabilitation, risk reduction, mental health, emotional health, and drug treatment. In addition, programs are offered to meet the needs of a variety of special populations such as veterans, inmates with disabilities, and those who are parents also receive specialized services.
In addition, the FBOP requires every literacy program must include a qualified special education instructor who meets the U.S. Office of Personal Management GS-1710 Education and Vocational Training Series Qualifications for a special education teaching position. This must be a full-time or part-time civil service or contract employee, who knows how to administer formal and informal tests, and helps other education staff meet the educational needs of low functioning inmates.
In accordance with the First Step Act of 2018 (FSA), the FBOP provides Evidence-Based Recidivism Reduction Programs and Productive Activities (EBRR/PA); eligible inmates may earn Federal Time Credits (FTC) for successful completion of these programs.

The following FBOP Program Statements, which are available electronically at http://www.bop.gov/, are applicable to this contract.

Program Statement 5300.21 – Education, Training, and Leisure Time Program Standards.
Program Statement 5350.28 – Literacy Program (GED Standard)
Program Statement 5200.05 – Management of Inmates with Disabilities

PERIOD OF PERFORMANCE

Upon availability of funds, the contract will consist of one base period: date of award to 12 months, and four consecutive 12-month option years.

SCOPE OF WORK

TEST DELIVERY

The assessment will be available as a computer-based test (CBT), and consists of a comprehensive battery of tests in the following areas:

- Cognitive abilities
- Academic achievement
- Oral language skills

The battery of test will be delivered in a digital format, with no physical materials required for shipping.

* Response booklets are needed for ten tests and allowed to be printed for free at the test site.

SCORING

The vendor will provide scoring and advanced analysis services for all assessments. The FBOP and it's institutions will have access to the reports which is the assessment scoring platform.

The assessment will provide automatic basal and ceiling rules, as well as automatic scoring.

Basal and ceiling rules are automatically implemented during the administration, which frees up time and attention for the examiner. Re-routing will automatically occur to ensure you establish the proper basal and ceilings. As an examiner, you can see your progress towards both the basal and ceilings throughout the administration of the test.

Correct and incorrect answers while administering the assessment shall be clearly identified for the examiner for quick and accurate scoring selections. For some tests, scoring is automatically implemented based on the examinee's response. As the examiner, you are always in control and can change the scores as needed, if you need to adjust based on examinee responses. At the end of every test administered, you will see the age and grade equivalent scores so you can make informed decisions about which tests to pull in or pass on an individual testing basis.

RECORDS AND REPORTS

The vendor will provide the FBOP with near real-time reporting about FBOP testers that have taken tests, as well as provide statistical reports, trend analysis, and empirical data via an interactive reporting system with on-demand and secure data retrieval. The contractor must ensure the availability of individual and aggregate assessment reports. All reporting must comply with applicable federal privacy regulations, including HIPAA and FERPA. The vendor shall ensure all data is securely stored and accessible only to authorized FBOP personnel. Upon contract completion or termination, all data must be returned to the FBOP and permanently removed from the contractor's systems.

The vendor will provide the cumulative statistical reports if requested. Statistical reports should be provided electronically allowing the FBOP to conduct further analyses, dissemination to the field, and employee training. As directed by the COR, the vendor may be periodically asked to generate special reports.

The interactive reporting system will provide an individualized prescriptive score report for each subject subtest and corresponding subject prerequisite regardless of outcome. This report will be used to assist FBOP instructors in developing data-driven instructional lesson plans, curriculums, and testing accommodation that will allow them to improve FBOP tester outcomes.

All tester accounts will be accessible from any FBOP test center. Tester account information (demographic, personal, contact, etc.) will be editable through self-service via the interactive reporting system or upon request (telephone or written) from FBOP field or Central Office staff, in no more than 48 hours of the request.

Tester records which include partial, or failed test results will be available to FBOP. Upon a tester's release from FBOP custody, the vendor will provide means for the tester's record to be available to be transferred to the tester or another entity responsible for the tester's custody. This will be at no extra

cost to the FBOP. Within 48 hours of notification from FBOP field or Central Office Administrative staff, the vendor will release a tester's record from FBOP and/or import tester's records into FBOP control.

The vendor will maintain permanent records of all Federal adults in our custody's test results, to include all test scores and administrations dating back to approximately 1954. Official copies of all records and test results will be maintained for an indefinite period of time, unless otherwise directed by the COR. All test records of Federal adults in custody are the property of the Federal FBOP.

The vendor will view and treat all scores and data as confidential information and will not release testing records unless requested by the COR. Due to security concerns, individual test records of adults in custody will not be shared as part of any database accessible to the public. The storage and exchange of records and personal identification information between the FBOP and the vendor will adhere to U.S. Department of Justice (DOJ) and FBOP information security requirements.

SUPPORT

The vendor will provide updates to test and supplies as they become available. Any testing artifacts required to administer the test will be provided to FBOP test centers. This does not include consumable materials (paper, pens, pencils, calculators, etc.).

The vendor will develop and provide examiner policy and procedure manuals, operating manuals, training materials, and other necessary materials (hard copies or electronic) with copyright permission for use at all test centers as these manuals and materials become available.

The vendor will provide technical and customer support during standard business hours to address issues with test materials, scoring platforms, or reporting systems. The contractor must provide a dedicated point of contact for the duration of the contract, as well as dedicate resource staff to specifically address issues associated with the assessment testing platform, to provide technical support, and address all issues with the testing environment. This support will include, but is not limited to, FBOP staff user account support and troubleshooting, record and reporting system, etc. No additional costs will be incurred for the resource staff. The vendor will dedicate one of their staff to address contract administration and any contract administration operations matters. The vendor will designate staff members to coordinate and process all matters (such as processing FBOP requests, preparing statistical reports, addressing test scoring, and test security issues, etc.).

PROFESSIONAL DEVELOPMENT

Approximately three times a year, the COR may request the contractor's resource staff members to provide specialized training (test administration, assessment scoring, etc.). These training sessions will occur at no additional costs to the FBOP.

Upon the COR's request, the vendor will provide the FBOP with the following:

- Provide an initial training process for all new test administrators (Special Education Teachers).
- Additional trainings could be developed (scoring, accommodations, etc.) for specific identified topics. The developed training material will be available for continued use by the Agency.

- Provide trainers (professional highly experienced trainers) to conduct/deliver a one-day (approximately 8 hours) of in-person assessment related training for FBOP Education staff at sites identified by the COR as needed.
    - The trainer will wear professional clothing while delivering the in-person training. The attire worn will also be appropriate for the environment in which the training will occur.
- Provide follow-up with Education staff related to training content.

CLOUD SERVICES

Any system that will connect to or be hosted in a non-FBOP cloud service must use cloud service providers (CSP) that have been independently evaluated by an authorized FedRAMP 3PAO (Third Party Assessment Organization) and are FedRAMP-certified. The CSP must provide the most current System Security Plan (SSP), Control Implementation Summary (CIS), Customer Responsibility Matrix (CRM), Security Assessment Report (SAR), and list of any open Plans of Actions and Milestones (POAMs) to the FBOP Chief Information Security Officer (CISO) for consideration. The CSP must receive an ATO from the FBOP Authorizing Official (AO) prior to use.

CLOUD APPLICATIONS – REQUIREMENTS FOR COTS AND CUSTOM DEVELOPED

Contractors must develop or provide administration and user guides for applications, whether the application is custom developed for the FBOP or is a Commercial Off the Shelf (COTS) product.
All applications must adhere to Section 508 accessibility standards.

CLOUD APPLICATIONS – CUSTOM DEVELOPED

The FBOP owns any and all source code generated for applications custom developed for the FBOP. The source code for any application custom developed for the FBOP must be delivered to the FBOP before the contract expires.

- Contractors shall use an Agile development strategy (or similar strategy) to enable rapid development with routine opportunities for stakeholders to review progress and provide feedback during the development process.
- Applications shall adhere to usability principles, plain language, and industry best practices.
- Applications shall interface with the FBOP's IdP using SAML2.0 or OAuth 2.0 to appropriately authenticate users and protect sensitive resources.
- Application data shall be made available via webservices that are built using REST APIs, with endpoints appropriately protected.
- Applications intended for deployment in the FBOP's cloud environment shall either be hosted in AWS GovCloud West or AWS GovCloud East, depending on the FISMA classification of the information contained in the system.
- Contractors shall identify exact cloud services and resources (i.e., Lambda, RDS types, EC2 instance types, etc.) that will be required to build the system and use the AWS cost estimation tool to provide a breakdown of the anticipated system cost.
- Contractors shall make necessary changes to the application, configuration, or cloud infrastructure/services script (i.e., IaC) if required by the FBOP cloud team.
- Contractors shall create CloudFormation scripts that will be used to build the Virtual Private Clouds (VPC) and infrastructure needed, and make necessary changes as identified by the FBOP cloud team.

Any exceptions to the above statements must be reviewed and approved by FBOP IT Leadership, and under no circumstances will any deviation from these statements that adversely affects the security of the FBOP IT environment or data be permitted.

SECURITY ASSESSMENT AND AUTHORIZATION COMPLIANCE

The FBOP will conduct an Assessment & Authorization (A&A) of the system before the Chief Information Officer's office issues an Authority to Operate (ATO) on the system.
Government project officers are responsible for ensuring their contractor-hosted or cloud-hosted applications are authorized to operate (ATO) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). This activity includes all planning, testing, and continuous monitoring activities associated with the system's lifecycle. **Most importantly, this means that the vendor is responsible for securing the resources to conduct required security testing, which for moderate or higher impact systems means using an independent third-party assessor qualified to conduct FISMA/FedRAMP audits**. The FBOP will not develop required FISMA/FedRAMP security documentation (except for assisting with the FIPS-199, e-Authentication, and Privacy Impact Assessment), or conduct any of the security testing for applications that are operated exclusively at contractor locations or hosted in the cloud. The extent of FBOP's support for exclusively contractor- and cloud-hosted systems is advisory only.
A&A is the methodology by which an organization establishes and then demonstrates a sound, risk-based security posture for a specific system. The A&A process establishes the extent to which a particular design and implementation meet a set of specified security requirements defined by the organization, government guidelines, and federal mandates into a formal authorization package. This authorization package is reviewed by the Authorizing Official (AO) and a formal declaration of an information system accreditation is either granted as an Authorization to Operate (ATO) or ATO with conditions or outright denial of authorization to operate. For more information about A&A requirements for federal IT systems, please see NIST SP 800-37 Rev 2 (https://csrc.nist.gov/pubs/sp/800/37/r2/final).
When this assessment is conducted, the vendor may be required to answer questions, to participate in the A&A process and potentially implement any information security changes necessary to facilitate receiving an ATO for this system. The system is required to meet or exceed specific and relevant security requirements identified and detailed in the Security and Privacy Requirements documentation.
Where a follow-up action against a person or the FBOP after an incident involves legal action (either civil or criminal), the system shall ensure that evidence can be collected, retained, and presented to conform to the rules for evidence in accordance with Federal rules of civil or criminal procedures.
The system and any/all electronic and information technology procured through this effort must be compliant with 29 U.S.C § 794d - Electronic and information technology (Section 508 compliance Amendment to the Rehabilitation Act of 1973) and the applicable accessibility standards at 36 CFR 1194. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at https://www.section508.gov/. Standards applicable to this requirement include Functional Performance criteria 1194.31 and Information, Documentation, and Support 1194.41.
Because of the above requirements, the contractor must include Information Systems Security Officer (ISSO) resources as part of the proposal to assist in the development of documentation for the ATO process. Such personnel should be experienced and familiar with writing control implementation statements so that security controls can be appropriately and promptly assessed. The length of the ATO process is dependent on the outcome of the quantity and quality of resources proposed for the solution.

PRIVACY AND RECORDS MANAGEMENT

All systems must be evaluated prior to ATT or ATO for privacy and records management requirements. An Initial Privacy Assessment (IPA) must be completed and if FBOP Privacy and Records Management Branch, and DOJ Office of Privacy and Civil Liberties (OPCL) determines that the system collects, processes, stores or disseminates personally identifiable information (PII), a Privacy Impact Assessment (PIA) must be done to evaluate the impact on the confidentiality, integrity, and availability of the system data. If required, the FBOP Office of General Counsel (OGC) will prepare a System of Records Notice (SORN) to be published in the federal register prior to system's deployment. All systems must complete a Records and Information Management Certification (RIMCert) evaluation regardless of Personally Identifiable Information (PII) status.
Contractor should be aware, for planning purposes, that the current FBOP ATO process can take 6 to 18 months to complete. The length of this time is dependent on the outcome of the IPA for the system.

SYSTEM INTERCONNECTIONS

DOJ requires that Components must identify all system interconnections, both external and internal to DOJ. A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. All interconnections from one information system to another system outside of the respective accreditation boundaries must have an approved Interconnection Security Agreement (ISA), and optionally a Memorandum of Understanding/Agreements (MOU/A). Both parties must mutually agree on terms and conditions and define expiration requirements or timelines. The agreements define how security will be maintained for the interconnection during its operation. Information systems are only permitted to interconnect with systems that have undergone a system authorization and have a current Authorization to Operate (ATO). If the Authorizing Official (AO) is the same for both interconnecting systems, an ISA or MOU/A is not required.

TECHNICAL REQUIREMENTS

Current Environment*

- Windows based clients with Edge/Chromium Browser access
- Client-side Environment:
    - Average concurrent test administered daily 350 - 400

* Note: Environment description subject to changes (versions, bandwidths, concurrent connections, etc.)

Key Business Objectives/Intended Results:

- A cloud-based, browser locked, managed testing platform (secure cloud based testing platform accessible through an agnostic locked browser.)) delivering testing to 121 sites nationwide.
- The vendor will provide interfaces (consoles, portals, etc.) and tools for administration of the HSE testing. Describe these interfaces and tools in detail.
- The testing platform will allow the government the capability to manage (add, delete, and edit) user accounts. Provide a bulk account creation and deletion process.
- The vendor will provide the government a single centralized backend administrative management interface. The backend administrative management interface will provide management from multiple levels by test center, complex, region, and agency. Describe the backend administrative management interface in detail.

- For exam delivery, the vendor will provide minimum/recommended system requirements (CPU, memory, disk storage capacity, etc.). Identify the requirements needed for the back-end HSE server environment, as well as any front-end client device requirements. Please identify any support for virtualized environments, dependencies or limitations that confine the deployment options to specific hardware types, operating systems, or deployment modes (e.g., appliances or endpoints).
- The vendor will provide details specific to user session average bandwidth usage/consumption based upon educational content type (audio, video, etc.). Additionally, indicate any hardware and/or software requirements for content test delivery (i.e., caching equipment, plug-ins, etc.) at customer location.
- The testing platform will support high availability configurations.
- In the case of migration, the vendor will provide a migration plan to ensure the continuity of user accounts, data, and progress.

Service Level Agreements (SLAs) will be adhered to for a testing platform:

- System Availability - 99% availability for users accessing the testing platform via the Internet 365 days/year, from 7:00 AM EST – 11:59 PM EST, 7 days/week.
- In measuring the availability, the platform must not be down, nor functioning at an unacceptable level of service, for more than 7 hours and 12 minutes (total) every month. Time associated with prior scheduled and approved maintenance must not be included in the downtime availability determination. Unacceptable level is defined as <98.9% availability for users accessing the system via the Internet 365 days/year, from 7:00 AM EST – 11:59 PM EST, 7 days/week.
- Written affirmations will be provided to the Contracting Officer identifying upgrades and patches that have been applied to the system or that are scheduled to be applied by COB on Monday for the prior week.
- Daily data backups of FBOP data will be conducted outside of service hours.
- Provide weekly report of testing platform usage to include bandwidth usage, general administrator logging, and inactive test center NLT COB on Tuesday for the prior week.
- Provide weekly report on numbers of simultaneous users and system response time NLT COB on Tuesday for the prior week.
- Provide monthly synopsis of problems encountered during the month, by NLT five (5) business days after the end of the month.
- For testing platform problems during hours of service (365 days/year, from 7:00 AM EST – 11:59 PM EST, 7 days/week) a qualified technician with access to the necessary systems, skills, and resources to troubleshoot should be available with a delay of no more than 10 minutes via telephone or email.
- For unplanned/unexpected testing platform outages during hours of service (365 days/year, from 7:00 AM EST – 11:59 PM EST, 7 days/week) platform experts with access to the necessary systems, skills, and resources to troubleshoot should be available with a delay of no more than 10 minutes via telephone or email for Education Branch and ICEN Support Team. For outages a target resolution of 24 hours or less depending on the corrective actions required to return the system to normal operations. Experts will be dispatched to be on-site at Washington D.C.
- The vendor cannot remotely access any government computers.
- Application event logging is required to include user transactions logs (system access, duration of general access, time spent per session, etc.). Application logs must be exportable to a syslog database for forensics and analysis. If the testing platform accesses external feeds or

integrations with third-party software or services, those interactions will be logged. The government reserves the right to deny any third-party software or services.

- The vendor will provide a secured isolated space/domain for the government (i.e., FBOP specific URL). Authentication controls must fail securely and deny access.
- The vendor's Learning Management System (LMS) will support multi-factor authentication for administrative users. Describe this process.
- The testing platform will provide the user self-service feature for password or account reset.
- The testing platform will provide a failed login attempt threshold with government notification.
- The vendor will provide a session management auditing feature(s). Describe the auditing features in detail.
- Credentials will be transported using a suitable protocol (minimal 256 bit) for encrypted link.
- Data at rest must be encrypted using FIPS 140-2 cryptographic libraries standards.
- Data transmitted over the FBOP network must use protocols that encrypt data as it traverses the network. Information systems must support the most current version of secure protocols and encryption standards and must be capable of being configured to prevent the use of non-secure protocols.
- Any information system that hosts a publicly accessible website and web services must only provide service through a secure connection (HTTPS) and must use HTTP Strict Transport Security (HSTS) to ensure this connection.
- The vendor's testing platform will provide a key management system (KMS). Describe the KMS in detail.
- The testing platform application will support binary digital signature by a publicly trusted Certificate Authority.
- The testing platform will use encryption for all application traffic. Please describe. Additionally, define all ports and protocols used for communication.
- Solution must be browser based and browser agnostic.
- Additional client software will not require additional licensing (i.e., OpenJava, Adobe Flash, etc.). If additional client software is required, the vendor will assume all cost. Please list additional client software required, if any.
- Isolation and segregation of all authenticated user accounts, to include data, and organizational units is required. Please describe.
- Public access is not authorized.
- The testing platform must provide 508 compliance. Please provide 508 VPATs with the proposal.
- The FBOP reserves the right to provide its own licensing for operating systems, databases, etc.

Place of Performance

The work will be performed at contractor site with meetings and collaboration with FBOP leadership and staff throughout. The program will be initially reviewed at FBOP headquarters (Washington D.C.) with further review of the program at select FBOP institutions. The number and locations of the latter will be determined by the COR depending on the approved platform design. Review of the program, at headquarters, will be completed within 180 days from development. If additional preparation time is needed, the contractor will submit a request to COR.

Security and Clearance Requirements

All required contractor personnel will have personnel security clearances commensurate with the Homeland Security Presidential Directive 12 (HSPD 12) for the highest level of information processed by the system(s) they use. The provisions of Department of Justice Order DOJ 1700.01, "Contractor Security Requirements", Federal FBOP of Prisons Information Security Program Statement 1237.16 and the Federal FBOP of Prisons Human Resource Management Manual 3000.03 will be followed to determine appropriate security clearance levels.
Contractor security clearances, including the submission of security clearance forms, etc., will be coordinated with the Technical Point of Contact (TPOC) prior to contract employee arrival at the FBOP institution. As determined by the TPOC and/or Human Resource Security Specialist, clearances may require one or all of the following:

- National Crime Information Center (NCIC) check
- DOJ-99 (name check)
- FD-258 (fingerprint check)
- Law Enforcement Agency checks
- Vouchering of Employers over past five years
- Resume/Personal Qualifications
- OPM-329-A (Authority for Release of Information)
- NACI check (if applicable)
- Urinalysis Test (for detection of marijuana and other drug usage)

Note: If it is determined that a urinalysis test is required, it will be administered at the closest FBOP site. If a test is positive for drug usage, the assigned individual(s) will be excluded from performance of work for this requirement, and subject to the same security requirements, the contractor will provide acceptable replacement staff.
The contractor will employ effective safeguards and security controls to ensure that information associated with the work is protected from loss, damage, computer viruses, or other destructive incidents. The safeguards employed should ensure that materials and services are secured in a manner that prevents tampering, sabotage, or other means of deliberate alteration. This provision applies to all FBOP information resources while under the control of the contractor. As referenced in the FBOP Policy Statement 1237.13, Information Security Programs, the contractor, while controlling FBOP information assets, will implement necessary safeguards, including administrative, physical, and personnel controls as outlined in said policy.
DOJ 2640.2F: The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position involves access to or development of any DOJ IT systems. By signing the contract document or beginning performance, the contractor agrees to this restriction.

Project Management and Coordination

The FBOP will appoint a Contracting Officer's Representative (COR) for this project. The COR is responsible for: receiving all deliverables; inspecting and accepting the services provided for this requirement 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; evaluates performance; and certifies all invoices/vouchers for acceptance of

the services furnished for payment prior to forwarding the original invoice to the payment office and a copy to the contracting officer.

The COR with oversight of this project will be:
NAME: TBD
ADDRESS:
Central Office Education Branch
Federal Bureau of Prisons
Washington, DC
PHONE NUMBER: TBD
EMAIL: TBD

The COR does not have the authority to alter the contractor's obligations under the contract action, direct changes that fall within the change clause, and/or modify any of the expressed terms, conditions, specifications, or costs of this agreement. If, as a result of technical discussions, it is desirable to alter/change the contractual obligations or requirements, the Contracting Officer will issue such changes in writing under signature.
The contractor will provide a Project Manager. The Project Manager will lead the overall execution of the activities in this SOW, including providing oversight of any tasks required by the SOW. The Project Manager will serve as the primary liaison between the Government and the contractor. Additionally, the Project Manager will ensure that:

- All contractor staff understands and work toward SOW requirements
- Tasks are staffed by appropriate, highly qualified personnel
- All project management issues are communicated to and coordinated with the COR

Status will be reported using at least bi-weekly project status reports and bi-weekly project status meetings. Document format should be Microsoft Office 2007 (or later) unless otherwise indicated. In addition, the contractor will:

- Arrange for the attendance, either in person or by conference call, of appropriate contractor personnel to address project issues
- Record minutes including, but not limited to, action items and responsible parties
- Provide meeting minutes within three (3) working days of the conclusion of the meeting.

TASK ADMINISTRATION

- **Discounts in Price Proposals:** To receive the highest quality solution at the lowest possible price, the Government requests all available discounts on offered by contractors for this requirement. Contractors are encouraged to offer discounts. When discounts are offered, proposals will clearly identify both the contract and the discount price for each rate being discounted. A copy of your contract rates will be enclosed with your proposal.

INVOICE SUBMISSION

- All invoices will be prepared in accordance with FAR clause 52.212-4 (g). The contractor will invoice the Government only for completed tasks. For all invoices, the contractor will provide invoice backup data, including labor categories, rates and quantities of labor hours.

- A monthly invoice for each task order will be submitted not later than five5 workdays after acceptance by the Government of the product, service, and/or cost item. A separate invoice for

each task order will be submitted on official company letterhead with detailed costs for each of the following categories:

- Total labor task charges
- Total invoice amount
- Prompt payment discount offered (if applicable)

- For Labor Hour tasks, the amount invoiced will include labor charges for actual hours worked and other actual expenses based upon contract rates and conditions, not to exceed the limits specified in the task order and that have been accepted by the Government.

- Payments will be made by Electronic Funds Transfer and in accordance with the Prompt Payment Act. The contractor will provide appropriate Electronic Funds Transfer information with its proposal. Invoices will be sent to the "Payment will be made by" address listed on the applicable delivery orders or, with respect to the guaranteed minimum for the base period, to the following:

  Federal FBOP of Prisons Central Office Business Office
  Washington, DC
  Telephone: TBD
  Email: TBD

- No charges will be paid by the Government, which are not specifically detailed in the individual task order, and specifically approved in the underlying contract.

- Invoices for final payment will be so identified and submitted when tasks have been completed and no further charges are to be incurred. These closeout invoices, or a written notification that final invoicing has been completed, will be submitted to the ordering agency within 30 days of task order completion. A copy of the written acceptance of task completion will be attached to final invoices. If the contractor requires an extension of the 30- day period, a request with supporting rationale will be received prior to the end of the 30-day period.

- Labor hours of subcontractors will not be billed at a rate other than the fully burdened hourly rates agreed to in the task order or at a rate specifically authorized for the task order as ODC's.

TASK ORDER FUNDING

- This award will be incrementally funded.

- The Contractor will notify the Contracting Officer and the COR, in writing, whenever the contractor has reasons to believe that the costs it expects to incur under this order in the next thirty (30) days, when added to all costs previously incurred, will exceed 75% of the total amount so far allotted to the order. The notice will state the estimated amount of additional funds required to continue performance for the period specified in the task order.

- The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount funded on this order by the Government; and the Contractor is not obligated to continue performance under this order or otherwise incur costs in excess of the total amount funded under this order.

- Contractor is put on notice that only the Contracting Officer has the authority to modify this task order. The Contractor will not accept direction to change the award.

PROJECT AND CONTRACT MANAGEMENT REQUIREMENTS

The contractor shall provide the planning, direction, coordination and control necessary to accomplish all project phases. The contractor shall designate a Project Manager (key personnel) who is responsible for the cost, schedule, and technical performance of the contract and who will serve as the Contracting Officer's central point of contact with the government. The Project Manager is not required to be full-time.

Kick-Off Meeting
The contractor shall attend a kick-off meeting between FBOP designated staff and the contractor team to discuss approach, policies, and procedure. The contractor shall provide a briefing on their technical approach for accomplishing results that meet the objectives of this task order to the Project Stakeholders.

Project Plan
The contractor shall provide a Project Plan that describes the technical approach, project personnel roles, organizational structure, available resources and management controls to be employed to meet the cost (monthly planned cost and hours for the period of performance), performance, schedule and milestones, communications, and quality requirements throughout the contract execution. The contractor must periodically update this Project Plan if there are any major changes in the work and/or schedule as bilaterally agreed to by the contractor and FBOP. The contractor must deliver a draft Project Plan within five (5) days after the kick-off meeting. The final Project Plan shall be due within ten (10) days after FBOP review and comments.

Project Schedule
Within the Project Plan, the contractor shall provide a Project Schedule for all tasks assigned under this contract and in line with the agile development approach. The contractor Project Manager shall ensure that the Project Schedule is developed and presented to the FBOP Project Manager/Contracting Officer Representative (COR) as part of the Project Plan. The Project Schedule shall identify all tasks, resources, and schedule. The Project Schedule shall become the schedule for the task and shall be maintained and updated weekly by the contractor for the duration of the contract/task to show progress completed. Tasks must have a short enough duration to update the project schedule on a weekly basis.

Progress Reports
The contractor shall provide written progress reports on a weekly and monthly basis for the duration of the project. These reports will be emailed to the COR and FBOP Project Manager. The Weekly Progress Report shall cover all work completed during the previous week and shall present the work to be accomplished during the subsequent week. The Weekly Progress Report shall be between one (1) and three (3) pages in length. The Monthly Progress Report shall be a summary of the prior 30 days' work and the subsequent 30 days' work to be accomplished. The Monthly Progress Report shall be no longer than ten (10) pages in length. These reports shall also identify any problems that arose and a statement explaining how the problem was resolved. These reports shall also identify any problems that have arisen but have not been completely resolved and provide an explanation. Additionally, status updates shall be provided during bi-weekly project status meetings.

Meetings/Meeting Minutes
The contractor shall provide administrative and technical support for meetings as required. The contractor shall coordinate scheduling and meeting notifications if required. The contractor shall prepare and provide briefing slides, handouts, agendas, meeting minutes, and other supplementary materials as required. All virtual meetings between contractor personnel and FBOP personnel must be conducted using the FBOP's collaboration/meeting system(s).

Contractor Background Clearances
All contractors must comply with DOJ/FBOP background clearance requirements before being permitted to do any work under a FBOP contract. All required documents must be submitted to the COR within 30 days upon contract start date. Contractors working remotely for the FBOP will be issued contractor user accounts and PIV cards. Contractors will be required to use government furnished equipment (computers) to access the FBOP network. To prevent loss of FBOP data, all email communication between contractor personnel and FBOP personnel must be conducted using the FBOP's email system. All pre-employment paperwork must be submitted within the first 30 days of the contract.

15. PROJECT DELIVERABLES

Deliverable	Format	Due	Acceptable
Project Kick-Off Meeting	Microsoft Teams	Project Start	Meeting between FBOP designated staff and contract team to discuss approach, policies and procedures. The contractor shall provide a briefing on their technical approach for accomplishing results that meet the objectives to Project Stakeholders.
Project Plan	Microsoft Word	5 days after kick-off	Describes the technical approach, project personnel roles, organizational structure, available resources and management controls to be employed to meet the cost, performance, schedule and milestones, communications, and quality requirements throughout the contract execution.
Project Schedule	Microsoft Word/Excel /MS Project (or other mutually agreed	10 days after kick-off	Within the Project Plan, the contractor shall provide a Project Schedule for all tasks assigned under this contract. The contractor Project Manager shall ensure that the Project Schedule is developed

	upon scheduling tool)		and presented to the FBOP Project Manager/Contracting Officer Representative (COR) as part of the Project Plan. This shall identify all tasks, resources, and schedule. The Project Schedule shall become the schedule for the task and shall be maintained and updated weekly by the contractor for the duration of the contract/task to show progress completed.
RACI Chart	Microsoft Word/Excel	10 days after kick-off	Outlines Contractor and FBOP responsibilities, including but not limited to project milestone tracking, UAT testing, meeting coordination, etc.
Progress Reports	Microsoft Word	Ongoing (weekly & monthly)	Written progress reports on a weekly and monthly basis for the duration of the project. These reports shall be emailed to the COR and FBOP Project Manager.
Risk Management Plan	Microsoft Word	45 days after award	Correct format, free of grammatical/clerical errors, on time.
Change Management Plan	Microsoft Word	45 days after award	Correct format, free of grammatical/clerical errors, on time.
System Management Plan	Microsoft Word	90 days after award	Correct format, free of grammatical/clerical errors, on time. Development Team and System Owner responsibilities, RACI (post development / post migration), etc.
Training Plan	Microsoft Word	90 days after award	Correct format, free of grammatical/clerical errors, on time.
*Agile Plan (Product vision statement, product roadmap,	Multiple	90 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time.

product backlog, release plan, sprint backlog, etc.)			Updated at end of each sprint.
Master Data Management Plan	Microsoft Word/Excel	90 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time. Updated at end of each sprint.
User Roles, Access, Permissions, and Security Plan, to include Security Information Assurance Package for Authority-to-Operate (ATO) to comply with NIST 800-53 security control assessment and authorization	Microsoft Word/Excel + standard NIST 800-53 format	120 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time. Updated at end of each sprint.
Training Library (how-to guides)	Multiple	120 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time. Updated at end of each sprint.
As-Built Documentation	Microsoft Word	120 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time. Updated at end of each sprint.

* If applicable to the project.