Federal Bureau of Prisons (FBOP)
Pre-Employment Screenings

1. Purpose
The purpose of this Statement of Work is to outline the requirements for providing comprehensive medical physical examinations for Federal Bureau of Prisons applicants through a self-schedule or walk-in service model. These examinations will include a medical assessment, vision screening, color vision testing, hearing evaluation, urinalysis, and fingerprint collection with same-day results provided to FBOP-designated personnel.

2. Scope of Services
The contractor shall furnish all labor, equipment, supplies, facilities, and qualified medical personnel necessary to perform the following services:

- **Medical Assessment**
  A licensed medical provider shall conduct a general physical examination to determine whether an applicant has any medical conditions that would reasonably prevent performance of the typical physical duties required for a law enforcement position, as defined in the "Physical and Medical Requirements of a Law Enforcement Worker."
    - If no disqualifying condition exists, the provider shall indicate the applicant is medically qualified. If the applicant is determined not medically qualified, the provider shall document the basis for that determination.
    - The contractor shall return all completed documentation to the Bureau of Prisons (BOP) on the same day the assessment is performed.
    - The contractor is responsible for completing all BOP-provided forms.
- Vision Test
  Measurement of visual acuity using accepted clinical methods. Results must indicate whether vision meets FBOP requirements.
- Color Vision Test
  Administration of a standardized color vision screening to confirm ability to distinguish colors as required for FBOP operational duties.
- Hearing Test
  Audiometric evaluation using calibrated equipment in accordance with OSHA or equivalent standards. Results will identify any hearing limitations relevant to the employee's role.
- **Urinalysis**
  Capable of collection and testing of urine specimens in accordance with Executive Order 12564. Testing must be conducted using laboratories and procedures certified by SAMHSA. Same-day results are required.
    - At a minimum, testing must be conducted for the following drug classes:
        - Marijuana
        - Fentanyl

    - Cocaine
    - Morphine, codeine, and other opiates
    - Amphetamines
    - Phencyclidine
- **Fingerprinting Services**
  Fingerprint collection compliant with FBI Identity History Summary Check standards. Requirements include:
    - Capture of all 10 rolled fingerprints plus plain impressions.
    - Use of FBI-certified live-scan equipment
    - Contractors must ensure proper applicant identity verification prior to fingerprint collection.
    - Fingerprints must be transmitted or provided in a format accepted by the FBI for Identity History Summary Checks.
    - Re-collection must be performed immediately at no charge if prints are rejected due to quality issues.

3. Service Delivery Requirements

- Scheduling
  Contractor shall provide options for self-scheduled appointments via an online platform or phone scheduling. Walk-in services must also be available during designated operating hours.
- Same-Day Results
  All examination components must be processed and delivered to FBOP-designated personnel on the same day the examination is completed. Results shall be presented in a secure, HIPAA-compliant format and the FBOP data must be destroyed
    - When same-day results are being transported outside of a secure area containing confidential FBOP Data, same-day results must be under the physical control of Contractor's staff with authorization to access the data.
- Contractor shall exercise due care and take reasonable precautions to protect and maintain FBOP Data against unauthorized use, access, disclosure, modification, and loss. Contractor acknowledges that FBOP is relying on the administrative, physical, and technical safeguards implemented by Contractor in permitting access to FBOP Data. Contractor's administrative, physical, and technical safeguards shall comply with all applicable laws, and applicable current privacy and security guidelines and/or standards issued by the DOJ OCIO and National Institute for Standards and Technology (NIST).
- If a cloud solution is utilized, it must be FedRAMP certified.
  Contractor shall not use, transfer, sell, or otherwise disclose FBOP Data for any commercial or personal purpose.
- Documentation
  Contractor shall supply a standardized results packet including:
    - Summary of medical assessment

- Assurance statement that applicant evaluation revealed no conditions substantially adversely affecting judgment, reliability, or trustworthiness
- Vision and color vision test results
- Audiometric findings
- Urinalysis report
- For fingerprinting, the contractor shall provide immediate confirmation of successful collection and submission, and supply results.
- Provider certification indicating completion of all required elements

4. Personnel Requirements

All services must be performed by appropriately licensed and certified professionals including, but not limited to:

- Physicians, nurse practitioners, or physician assistants for medical assessments
- Laboratory technicians trained in specimen handling and testing
- Fingerprint technicians trained in FBI fingerprint capture standards

5. Facility Requirements

The contractor's facility must:

- Meet all federal healthcare standards
- Provide private spaces for examinations and specimen collection
- Maintain calibrated equipment
- Maintain FBI-certified live-scan fingerprint equipment

6. Compliance

All services must adhere to:

- Federal Bureau of Prisons medical standards
- HIPAA privacy regulations
- OSHA audiometric requirements
- Applicable healthcare regulations
- All FBI technical and procedural standards for fingerprint collection
- Contractor shall comply with the policies, standards, and guidelines of the DOJ OCIO and all applicable state and federal laws in its treatment of FBOP Data, including, but not limited to,
  - 5 U.S.C. § 552a – Privacy Act of 1974 (Pub. L. 93-579)
  - FIPS PUB 140-3 – Security Requirements for Cryptographic Modules the Health Insurance Portability and Accountability Act (HIPAA),
  - Pub. L. 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH);
  - 44 U.S.C. § 3551 et seq. – Federal Information Security Modernization Act (FISMA) of 2014 (Amended by Pub. L. 113-283, 128 Stat. 3073)
  - 28 U.S.C. § 534 – Acquisition, preservation, and exchange of identification records and information

- OMB Circular A-130 – Managing Information as a Strategic Resource, 81 FR 49689 (July 28, 2016), including Appendix I (Responsibilities for Protecting and Managing Federal Information Resources)
- OMB Memorandum M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information
- DOJ Order 0904 – Cybersecurity Program
- DOJ Policy Statement 0904.01 – Cybersecurity Program Policy

7. Performance Measures

Contractor performance will be evaluated based on:

- Timeliness of same-day results
- Accuracy and completeness of documentation
- Professionalism and credentialing of staff
- Employee satisfaction and service accessibility
- Compliance with all stated requirements
- METHOD OF PERFORMANCE: The services to be provided are for non-personal medical services, as defined in the Federal Acquisition Regulations (FAR), Part 37.101, under which the contractors are not employees, but contractors. The Government may evaluate the quality of professional and administrative services provided but retain no control over the professional aspects of services rendered. The vendor is required to indemnify the Government for any liability producing act or omission by the vendor, its employees and agents occurring during the period of performance. These services and the performance of these services will be verified by the designated COR.

8. Period of Performance

The contractor shall provide services for the duration defined in the award contract, with options for renewal as determined by the FBOP.

9. Deliverables

- Completed physical examination results for each employee
- Fingerprint collection documentation and submission confirmation
- Immediate notification of any medical findings requiring urgent attention
- Data will be encrypted when shared electronically.
- In the event Contractor fails to comply with any material term of this contract, FBOP shall have the right to take any and all actions to remedy such failure and its effects that FBOP, in its sole discretion, deems reasonable under the circumstances. Any costs, fees, or expenses, including legal costs, incurred by FBOP as a result of Contractor's failure to comply with the terms of this contract shall be recoverable from Contractor. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law and to legal remedies available to parties injured by unauthorized disclosure.

- If FBOP data that are identifiable to a private person are transmitted between authorized contractors, the contractor will encrypt any media used to transmit the data before distributing it to either party. The Contractor will also ensure that any sensitive data stored offsite from its facilities is encrypted ("data-at-rest"), in accordance with OMB Memoranda 01-05 and 06-16 and DOJ Order 0904.

  The Contactor will ensure that any readable computer data extracts from the FBOP holding sensitive information are erased within 90 days unless their use is still required in accordance with OMB Memorandum M-17-12 (January 2017) and the DOJ IT Security Rules of Behavior for General Users (September 2025). As well, Contractors may only retain sensitive information during the project period only as long as it is required to complete the approved project activities, including data collection, analysis, and verification, associated with the uses and deliverables described in this agreement. After such need or project has expired, the data must be erased from contractor systems and media.

10. Technical Standards for Acquisitions of FBOP IT Systems and Peripherals
DEFINITIONS
Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.)
Peripheral Device: Any auxiliary device that connects to and works with a computer or information system in some way. Examples of peripherals are image scanners, tape drives, microphones, loudspeakers, and webcams.

1. INFORMATION SYSTEM REQUIREMENTS
1.1. APPLICABILITY
All information systems deployed within the FBOP, or on behalf of FBOP to include contractor built and operated on-prem, private cloud systems, or government cloud, must be developed to include support for the standards detailed in this section to the greatest extent possible regardless of whether the system is connected to the FBOP's administrative network (BOPNet). All systems will be evaluated prior to acquisition and/or deployment to determine that each system supports the technical standards contained in this section. Approval to connect to BOPNet will not be granted to any system that cannot support these standards unless a waiver has been granted by the CIO.
Additionally, all systems must acquire an Authority to Operate (ATO) prior to use, and an Authority to Test (ATT) prior to system testing. Testing will not leverage live data (must use data created for the sole purpose of verifying functional capability and contain neither FBOP nor FBOP user information). A pilot, if needed, will also be performed without the use of live data. All the system environments, including development, test, quality assurance, integration, production, and any other environment related to the system, must reside within the authorization boundary.

2. OPERATING SYSTEMS, DATABASES, AND APPLICATIONS

2.1. OPERATING SYSTEMS AND DATABASES

All systems shall be developed to use FBOP standard workstations, laptops, and servers with versions of operating systems and databases that are currently supported and will continue to be supported by the manufacturer/developer for at least three years after the FBOP system goes live. Any system that requires operation on an operating system and/or database that is no longer supported or will be approaching its end-of-life or the end of extended support date before the contract expires, is prohibited from being installed unless a waiver is granted by the CIO.

All devices must have Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Category I and Category II settings applied. Workstations and laptops with Windows operating systems must have DISA STIG settings applied for the versions of Windows currently in standard use in the FBOP. Servers, workstations, laptops, and other devices running non-Windows operating systems must be approved for use by the CIO prior to acquisition and must be the latest supported versions by the vendor. If a DISA STIG exists for any non-Windows operating system, the operating system must be configured in accordance with that DISA STIG.

Any system requiring on-premises installation of servers and/or server applications will require installation on FBOP-provided virtual servers. All software, applications, and server appliances must receive approval for use from the FBOP Information Technology and Data Division (ITDD) prior to installation.

2.2. APPLICATIONS

All systems on the FBOP network shall be capable of using a FBOP standard image for workstations. Systems shall be developed to minimize the installation of new applications directly onto workstations. Systems that require a client application be installed on workstations are strongly discouraged.

Web-based applications shall be installed on standard FBOP servers running FBOP-approved server operating systems and meet the following requirements:

i. Support TLS (non-deprecated version);
ii. Be browser-agnostic;
iii. Not require browser plug-ins, helper objects, specific ActiveX controls, or Java dependencies on the client.

All applications must be able to operate with the latest version of any supporting applications or services required to run that application (i.e., Java, Apache, IIS, etc.).

2.3. AUDITING/LOGGING

All operating systems and/or applications must be capable of auditing events and maintaining logs with sufficient information to be able to account for the actions of individual users and record system events and processes.

3. IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

To comply with Homeland Security Presidential Directive 12 (HSPD-12), all information systems must use a centralized directory for identification, authentication, and authorization to control, provision, and de-provision access to those systems. To connect to the FBOP network, all information systems must be capable of supporting Lightweight Directory Access Protocol (LDAP v3 or successor).
Systems that cannot support either a FBOP directory service or DOJ federated service and require the management of a separate credential store for identification, authentication, and authorization are prohibited.
Each system user must be uniquely identified. Access to information is controlled using a "Least Privilege" role- or assignment-based methodology that provides the user with only the information and access required to perform his/her duties and nothing more. Systems must be capable of tiered-role privileges that distinguish between users and administrators and their authorized functions.
The federal government has implemented a Zero Trust security model to enforce least privilege per-request access decisions in information systems and services. Therefore, authentication to the system must be facilitated via the use of multi-factor authentication and access to the data controlled via role-based access.

4. ENCRYPTION

4.1. DATA AT REST

All information systems that store data must have the capability to encrypt the drives on which the data is stored using FIPS 140-2 compliant encryption. If the system cannot support encryption of system drives, it must be approved for use by the CIO prior to acquisition and use.

4.2. DATA IN MOTION

All information systems that transmit data 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.

4.3. PUBLIC FACING WEBSITES

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.

5. ENDPOINT SECURITY AND VULNERABILITY MANAGEMENT

All networked information systems shall be capable of being managed through an approved endpoint security and management application and be fully operational while being scanned for security vulnerabilities without disruption of service. All networked systems shall also be capable of being patched using a centrally managed patch management application.
Computer workstations, laptops, tablets, servers, and other computing devices using an operating system must employ anti-virus software protection. Anti-virus software and virus definition files must be updated with the most current versions and the anti-virus software must be configured to:

i. Begin protection when the devices are powered on;
ii. Scan daily;
iii. Check all files processed by the system in real time.

6. NETWORK STANDARDS AND PROTOCOLS

6.1. NETWORK STANDARDS AND APPROVED PROTOCOLS

Information systems must meet the following network standards to be deployed on the FBOP network:

i. Supports IPv4/v6 Dual Stack and provides full and equal functionality when utilizing IPv6 as when using IPv4;
ii. Does not require or enable wireless of any type (Wi-Fi, Bluetooth, 3G/4G, etc.) unless an exception is granted by the CIO and is implemented per FBOP and DOJ guidelines;
iii. All physical devices that make up the system must have a single network connection, only one IPv4 address, one Globally Unique IPv6 address, and not be capable of routing;
iv. If internet accessible, can transmit traffic thru a proxy server to access the internet;
v. Does not require direct inbound connections from the public internet;
vi. Does not allow out-of-band access (no modems, etc.);
vii. Does not require media converters;
viii. Does not directly connect to other IP networks;
ix. Does not use IPv4 Multicast;
x. Cabling is IEEE Gigabit standard compliant;
xi. Power over Ethernet (POE) devices are IEEE 802.3af compliant;
xii. Cannot act (or is disabled from acting) as a DHCP server.

6.2. NON-SECURE PROTOCOLS

In accordance with current NIST standards, non-secure protocols must be disabled and not planned for use. The information system must have the capability of disabling any non-secure protocols including, but not limited to, the protocols listed below:

i. Telnet
ii. FTP
iii. SNMP v1/2
iv. HTTP

7. 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.

7.1 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.

7.2 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.

8. MEDICAL SYSTEMS

Medical systems must comply with standards published by the Office of the National Coordinator for Health Information Technology (ONC) in regard to data access, storage, and reporting. Medical software/systems must be Heath Insurance Portability and Accountability Act (HIPAA) compliant. The contractor shall provide a HIPAA compliance plan and designate a compliance officer with the required extensive background/training to satisfy this requirement. As part of HIPAA compliance, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI the contractor creates, receives, maintains or transmits;

- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by the contractor's workforce.

9. MOBILE APPLICATIONS

Mobile applications must be designed using HTML5 or operate natively on a version of the Android operating system currently being supported by industry with security patches.

10. PERIPHERAL REQUIREMENTS

10.1 LOCALLY ATTACHED PERIPHERALS

Peripherals that are locally attached to standard FBOP workstations must:

i. Not be shared on the network;
ii. Not require software to operate that requires access to the internet or other network resources;
iii. Not require software to operate that requires older versions of software to operate such as Java;
iv. Not broadcast wireless signals (i.e., Bluetooth, WiFi, etc.);
v. Not require a change to the workstation local security policy to operate.

10.1.1. LOCALLY ATTACHED PRINTERS AND SCANNERS

Locally attached printers and scanners must have 64-bit drivers and cannot be shared to workstations other than the workstation to which it is directly connected.

10.2. NETWORKED-ATTACHED PERIPHERALS

Peripherals that must connect directly to the FBOP network shall be part of a larger system or sub-system authorized to operate on that network. Each system or sub-system must provide controls to the peripherals attached to the network that comply with the system standards detailed above or provide mitigating controls for peripherals that cannot meet a system standard.

10.2.1. MULTI-FUNCTION DEVICES AND NETWORKED PRINTERS

All multi-function devices (MFD) and networked printers must be capable of being configured in accordance with the Multifunction Device and Network Printers DISA STIG. MFDs must be capable of supporting PIV authentication either directly or via a peripheral attachment/software but are not required to use PIV authentication at this time.

11. 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.

12. 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.

13. 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.

14. 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. 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 communications between contractor personnel and FBOP personnel must be conducted using the FBOP's email system.

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 upon scheduling tool)	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 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, product backlog, release plan, sprint backlog, etc.)	Multiple	90 days after award, continuously updated	Correct format, free of grammatical/clerical errors, on time. 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.

PRICING / SCHEDULE OF ITEMS:

Pricing Methodology- The contract rates for service will be on a per applicant basis. Price quotes shall be inclusive of all charges (i.e., wages, insurance, supplies, transportation services, personnel, overhead, profit, etc.) necessary to provide service. Minimal processing time required to enter/exit the institution should be reflected in contract pricing.

Quoters should submit a completed copy of the Schedule of Items inclusive of base and option year pricing. Evaluation of price quotes will be inclusive of options and quoters may offer varying prices for the options. Finally these estimates are not a representation to a quoter that the estimated quantities indicated will be required, or that condition affecting requirements will be stable or normal. Services will be ordered via issuance of individual calls/orders placed against a resultant contract.

Contractor-provided clinic services shall include, as part of their unit pricing, all labor, administrative effort, and time required to complete the Medical History Report Form provided from the BOP for each candidate. Clinics are expected to incorporate this activity into their quoted price for medical assessments and related screening services. No separate or additional reimbursement will be provided for completing this form, and all associated costs must be fully burdened within the clinic's submitted pricing. This ensures consistent, all-inclusive pricing for pre-employment medical evaluations conducted under the contract.

The resulting award will provide two categories of pre employment screening services, each delivered through commercially available community-based facilities. The contract will include:

001: LEO Package- Comprehensive Screening Package for Law Enforcement applicants This package includes basic medical screening services (medical assessment, vision testing, color vision testing, and hearing testing), urinalysis drug testing, and biometric fingerprint collection.

002: Non-LEO Package- Limited Screening Package for Non-Law Enforcement applicants. This package includes urinalysis drug testing and biometric fingerprint collection.

Base: Effective Date of Award (EDOA) through 12 months

001 – LEO Package: Estimate of 5,000 applicants x $ _____ each.

002 – Non-LEO Package: Estimate of 5,000 applicants x $ _____ each.

****

Option 1: 13 months from EDOA through 24 months

001 – LEO Package: Estimate of 5,000 applicants x $ _____ each.

002 – Non-LEO Package: Estimate of 5,000 applicants x $ _____ each.

****

Option 2: 25 months from EDOA through 36 months

001 – LEO Package: Estimate of 5,000 applicants x $ _____ each.

002 – Non-LEO Package: Estimate of 5,000 applicants x $ _____ each.

****

Total estimated value of services: $ _____

Medical History Report
-To Be Completed by Applicant-

Last Name	First Name	Middle Initial	Date of Birth [MM/DD/YYYY]

List Medication (s)

Have you ever had or have now	Yes	No	Have you ever had or have now	Yes	No
1. Headaches?			12. Tumor, cancer, or organ transplant?		
2. Dizziness/Fainting?			13. Neck or back pain?		
3. Trouble smelling?			14. Painful, swollen, or unstable joints?		
4. Skin disease?			15. Broken bones?		
5. Pain/Pressure in the chest?			16. Foot or ankle pain?		
6. Cardiovascular disease?			17. Diabetic low blood sugars?		
7. High/Low blood pressure?			18. Any mental health/psychiatric condition?		
8. Trouble breathing?			19. Suicide attempt?		
9. Head injury?			20. Been hospitalized for any medical or psychiatric care?		
10. Epilepsy or seizure(s)?			21. Been denied employment for any medical or psychiatric reason(s)?		
11. Hernia?			22. Had any surgeries?		

Explain all "Yes" responses

READ THE FOLLOWING CAREFULLY BEFORE SIGNING THIS DOCUMENT
A false answer to any question on this form or portion thereof may be the grounds for not employing you, or for dismissing you after you begin to work, and may be punishable by fine of up to $10,000 or imprisonment of up to five years or both.

CERTIFICATION
I certify that all the answers and statements made on this form are true, complete and correct to the best of my knowledge and belief and are made in good faith.

Signature of Applicant	Date [MM/DD/YYYY]

Applicant Physical Exam Report
-To Be Completed by Medical Provider-

Last Name	First Name	Middle Initial	Date of Birth [MM/DD/YYYY]

Body Measurement and Vital Signs							
Height (in)	Weight (lbs)	BMI (kg/m^2)	Temperature (F)	Blood Pressure (mmHg)	Resp. Rate (per min)	Pulse Rate (per min)	
Audiogram Results	500 Hz	1000 Hz	2000 Hz	3000 Hz	4000 Hz	6000 Hz	8000 Hz
Right							
Left							
Hearing Aid	☐ Yes	☐ No					

Vision (Best Distant Vision)			Color Vision
Right	20/		
Left	20/		

Physical Examination		
General	☐AOx3 ☐NAD	Positive Finding(s):
HEENT	☐NCAT ☐CN II-VII intact ☐ Normal TM R/L ☐ No nasal obstructions ☐Clear oropharynx ☐ Mallampati	Positive Finding(s):
Cardiovascular	☐ RRR ☐ No m/r/g ☐ Normal S1 and S2 ☐ Palpable radial pulses ☐ Palpable DP pulses	Positive Finding(s):
Pulmonary	☐ Non-labored breathing ☐ No accessory muscle use ☐ CTAB ☐ No wheezes, rales, rhonchi	Positive Finding(s):
Abdomen	☐ Soft and NTTP ☐ Normal BS ☐ No rebound or guarding ☐ No abdominal hernias	Positive Finding(s):
Genitourinary	☐ No inguinal hernias detected	Positive Finding(s):
Musculoskeletal		
Neck	☐ Normal ROM ☐ Normal MS ☐ NTTP	Positive Finding(s):
Back	☐ Normal ROM ☐ Normal MS ☐ NTTP	Positive Finding(s):
Upper Extremities	☐ Normal ROM ☐ Normal MS ☐ NTTP ☐ Sensation intact ☐ Normal DTR triceps/biceps/brachioradialis b/l	Positive Finding(s):
Lower Extremities	☐ Normal ROM ☐ Normal MS ☐ NTTP ☐ Sensation intact ☐ Normal DTR patellar/plantar b/l	Positive Finding(s):
Other Neurologic	☐ Normal gait ☐ Normal tandem walk ☐ Negative Romberg test ☐ No pronator drift ☐ Normal finger-to-nose test/heal-to-shin test	Positive Finding(s):
Dermatologic	☐ Normal intact skin on face, neck, arms	Positive Finding(s):

Physician Note (s)

Based on this general medical examination, and with reference to the standard medical and physical requirements for law enforcement positions, the examinee is:

☐ **Medically Qualified** - No medical condition identified during this exam would prevent the applicant from performing the typical physical duties of a law enforcement position.	☐ **Not Medically Qualified** - A medical condition identified during this exam may prevent the applicant from performing the typical physical duties of a law enforcement position.
Examining Clinic	**Date of Examination [MM/DD/YYYY]**
Name of Physician	**Signature of Physician**

PHYSICAL AND MEDICAL REQUIREMENTS OF A LAW ENFORCEMENT WORKER

Incumbents of positions in correctional institutions are considered law enforcement officers and are required to meet the following physical and medical requirements:

1) Be alert and able to recognize and respond effectively to emergencies at all times
2) Be mentally and emotionally stable based on history and physical examination
3) Be free of active skin and pulmonary diseases that could be spread by routine means
4) Walk for up to one hour
5) Stand for up to one hour
6) See a human figure at a distance of one-fourth of a mile
7) See a target at a distance of 250 yards; (visual acuity of at least 20/30 in one eye)
8) Hear with or without a hearing aid, in at least one ear measured by normal findings of < 40dB in 500, 1000, and 2000 Hz range
9) Perform the following self-defense movements against resistance
    a. Overhead reach by Upper Extremity in all planes bilaterally
    b. Abduction and Adduction of Upper Extremity at Shoulder bilaterally
    c. Supination of Wrist
    d. Flex Forearm, Arm, Wrist, Back, Hip, Knee, Ankle
    e. Extend Forearm, Arm, Wrist, Back, Hip, Knee, Ankle
    f. Pivot on Lower Extremity
    g. Twist Back and Hip
    h. Squat
    i. Kneel
    j. Fall onto Back/Side from Standing position
10) Running an extended distance (at least ¼ mile)
11) Drag a body an extended distance (75 pounds for 694 ft)
12) Carry a stretcher with one other person
13) Smell smoke and drugs
14) Climb stairs (3 flights up and down)
15) Lift objects weighing 25 pounds
16) Medically safe to wear tight fitting respirators