



The mission of the Baltimore City Information Technology Office is to “provide sustainable infrastructure and technology to support and enhance City agencies, communities, and businesses, and to meet City and mayoral goals.”

1. Description of the Project

The Baltimore City Office of Information & Technology (“BCIT”) is seeking a qualified Contractor to provide a comprehensive, end-to-end Software-as-a-Service (“SaaS”) solution for the Municipal Identification Card Program. The solution shall include (1) a configurable technology platform; (2) accompanying hardware and consumables necessary to support fixed-site and mobile card issuance; and (3) professional services necessary to configure, implement, test, deploy, maintain and support the solution.

The selected Contractor shall serve as the single point of responsibility for delivering a fully functional system, including software, configuration, integration, deployment, and ongoing support services.

The selected Contractor shall support the City in producing identification cards with enhanced security features; implementing procedures and mechanisms aligned with industry-standard document authentication and identity verification practices, including applicable federal, state, and local guidance; developing and delivering technology-related training programs for City staff, partners, and authorized users; and supporting the issuance of identification cards in a manner consistent with Baltimore City Code requirements, including the prohibition on retaining originals or copies of applicant identity or residency documents and the prohibition on retaining or creating lists of applicant or cardholder names or addresses. Any retained data must be de-identified and incapable of being linked to a specific individual by name, with a fraud-prevention allowance for descriptive or demographic data tied to card number.

The selected Contractor shall also provide technology-related organizational change management support necessary for successful implementation and adoption of the solution, including role-based training, training materials, user guides, job aids, system demonstrations, train-the-trainer support, go-live readiness support, hypercare support, and input to system-related FAQs and communications.

The selected Contractor shall coordinate with the City and any separately procured Program Development Contractor to translate approved program policies and operating procedures into system workflows, configurations, reports, user roles, training materials, and operational support processes.

The Mayor and City Council of Baltimore passed legislation in 2016 establishing the Program. Government-issued photo identification is essential to full participation in civic, economic, and



community life. Some of the City's most vulnerable residents face significant obstacles when attempting to obtain identification because of immigration status, unstable housing, gender identity or other barriers. Municipalities across the United States, such as Chicago, Philadelphia, New York, Detroit, and San Francisco, among others, have implemented municipal identification programs to address similar needs. In Baltimore, BCIT will administer the Program with the assistance of all City agencies.

The Program is designed to be welcoming and inclusive to all Baltimore City residents, without regard to race, national origin, religion, sex, sexual orientation, gender identity, disability, or immigration, housing, or financial status.

2. Anticipated Timeline

The term of this contract will be for a period of three (3) years with three (3) one (1) year renewal options.

1. REQUEST FOR PROFESSIONAL SERVICES PROPOSAL # SRV0919_001 Municipal ID Card Program Technology Solution	2. ISSUE DATE: May 13, 2026	MINORITY PARTICIPATION GOALS: Waived
---	--	--

3. ISSUED BY: Baltimore City Information and Technology 401 E. Fayette Street 3 rd Floor Baltimore, Maryland 21202	4. SUBMIT QUESTIONS & PROPOSALS TO: BCIT CONTRACTS Email Address: BCITContracts@baltimorecity.gov
5. QUESTIONS DUE: May 29, 2026, By 4:00 PM EST ALL QUESTIONS MUST BE SUBMITTED IN WRITING AT THE EMAIL ADDRESS IDENTIFIED IN ITEM 4 ABOVE. NO PHONE CALLS WILL BE ACCEPTED.	6. PROPOSALS DUE: June 15, 2026, By 4:00 PM EST

3. Method of Award

The City of Baltimore anticipates awarding a single contract to the responsible and responsive Contractor whose proposal is determined to be the most advantageous to the City, taking into



consideration technical qualifications, experience, proposed approach, cost, and other evaluation factors as set forth in this professional services solicitation.

The City reserves the right to make an award based on initial proposals received, without discussions, or to conduct discussions, request best and final offers (BAFOs), and/or make multiple rounds of evaluation as deemed necessary.

The City further reserves the right to reject any or all proposals, waive minor irregularities, and to make no award if it is determined to be in the best interest of the City.

4. Evaluation Criteria

(1) Technical & Implementation Approach, (2) Management Approach, (3) Past Performance, (4) Compliance and Security, (5) Price. The City of Baltimore intends to award a single contract to the Contractor whose proposal represents the best value as the expected outcome in response to the Statement of Work requirements. Contractor's capabilities to deliver high quality services, in consideration of their expertise and experience, will be assessed. The Evaluation Committee will evaluate and score only those proposals determined to be responsive and complete, including all required sections and documentation as specified in this solicitation. The Evaluation Committee reserves the right to recommend award to a Contractor whose proposal is not the lowest priced or highest technically rated, if such proposal is determined to provide the best overall value to the City of Baltimore. In making this determination, the Evaluation Committee may consider trade-offs between price and non-price factors in accordance with the evaluation criteria set forth in this solicitation.

(4.1) Technical & Implementation Approach – 40 Points

The Contractor shall describe its technical solution and implementation approach for delivering a comprehensive Software-as-a-Service (SaaS) platform and supporting hardware for the Municipal Identification Card Program. The proposal must demonstrate a clear, feasible, and technically sound approach to system configuration, deployment, integration, and operational functionality. All configurations, workflows, and customizations developed under this contract shall be owned by the City.

At a minimum, the Contractor shall address the following:

Technical Solution & System Capabilities

- Describe the proposed SaaS solution, including core system functionality, features, and capabilities. The Contractor shall explain how the solution meets the requirements of the Program, including user workflows, data capture, card issuance, reporting, and system administration. Describe how the proposed solution will meet accessibility and language access requirements for public-facing and staff-facing components, including appointment scheduling, applicant-facing workflows, instructions, error messages,



reporting interfaces, training materials, and support content. The Contractor shall identify applicable accessibility standards, language capabilities, and any City responsibilities for translation, content updates, or accessibility testing.

Required Solution Architecture Package

- Provide a proposed Solution Architecture Package that includes: logical architecture diagram; data-flow diagram showing where applicant data is captured, processed, transmitted, displayed, printed, temporarily cached, and destroyed; hosting model and cloud provider; environment separation; fixed-site and mobile-site connectivity model; endpoint and device management approach; administrative roles and access model; API architecture, if applicable; and system dependencies, assumptions, and City responsibilities.

System Configuration & Deployment Approach

- Describe how the solution will be configured and deployed, including environment setup, system configuration, deployment sequencing, readiness for production use, cutover approach, and transition from implementation to operations. Include any assumptions, dependencies, or prerequisites, City responsibilities, and decisions required from the City.

System Integration & Data Management

- Describe how the solution will integrate with existing City systems, and third-party systems, if applicable, including data exchange, APIs, and interoperability, validation, and data integrity controls. Describe approach to data migration, validation, and data integrity. Explain how data is processed, retained, de-identified, destroyed, or excluded from retention in accordance with applicable City requirements.

Hardware & Device Functionality (if applicable)

- Describe the proposed hardware components, including device capabilities, configuration, security, inventory controls, maintenance, replacement approach, and how hardware integrates with the SaaS platform to support program operations (e.g., enrollment, identity verification, card production at fixed and mobile sites).

Issue Resolution & System Support (Technical Perspective)

- Describe the technical process for identifying, diagnosing, escalating and resolving system-related issues, including system errors, outages, device failures, API or validation service issues, security incidents, and performance issues. The Contractor shall describe its support model, system support capabilities and SLAs such as uptime expectations, maintenance windows, and service availability.

Performance, Reliability & Scalability

- Describe how the solution ensures system reliability, performance, and scalability to support current and future program needs. Include system capacity, expected response times, peak-volume handling, failover approach, disaster recovery approach, and ability to scale with increased usage or additional issuance locations.



Security Testing & Privacy Verification

Describe the approach to penetration testing prior to go-live and on a recurring basis thereafter. The initial pre-go-live test shall be conducted by a qualified team independent of the development team. The scope shall cover the complete solution including verification that no-retention and PII purge mechanisms function as designed. All critical and high-severity findings must be remediated before production deployment.

System Monitoring & Reporting Capabilities

- Describe built-in tools for monitoring system performance, operational activity, and generating reports. Reporting and audit capabilities must be designed to support operational visibility (e.g., dashboards, usage metrics, audit logs) without retaining prohibited applicant or cardholder information.

Municipal ID Validation API / Validation Service requirement

- The solution shall provide a secure validation capability that allows City-approved systems or partners to verify whether a Municipal ID card number is valid and active. The validation capability shall return only a limited response, such as valid/invalid, status code, and response timestamp. It shall not return name, address, date of birth, photo, document information, demographic information, issuance site, appointment details, or any other personally identifiable information. At a minimum, the validation service shall support token-based or OAuth2-equivalent authentication, IP allowlisting or equivalent access restriction, rate limiting, API key revocation, audit logging without PII, test/sandbox access, and current technical documentation.
- The Validation API shall support use by City agencies and employees to fulfill their obligation to accept the Municipal ID Card as proof of identity and residency.

Technical & Implementation Approach 40 points

- Meets requirements 33 to 40 points
- Meets most requirements 25 to 32 points
- Meets some requirements 17 to 24 points
- Meets minimal requirements 9 to 16 points
- Meets 1 requirement 1- 8 points
- Does Not Meet requirement 0 points



(4.2) Management Approach 20 points

The Contractor shall demonstrate a clear, well-structured, and feasible management approach for the successful implementation and ongoing operation of the Municipal Identification Card Program. The proposal must reflect a strong understanding of the operational requirements and present a practical approach to delivering services efficiently and effectively.

At a minimum, the Contractor shall address the following:

- **Understanding of Requirements**
Demonstrate a thorough understanding of the technical, operational, and programmatic requirements outlined in this solicitation, including SaaS implementation, hardware deployment, and ongoing support needs.
- **Overall Management Approach**
Describe the approach to planning, coordinating, and managing all aspects of the project, including governance structure, roles and responsibilities, and communication protocols.
- **Implementation Strategy & Work Plan**
Provide a detailed implementation plan, including key phases, milestones, timelines, and dependencies. The plan should demonstrate how the Contractor will ensure timely and successful deployment of the solution. The Contractor shall describe its approach to developing and maintaining an integrated City-Contractor project schedule that accounts for Contractor activities, City activities, dependencies, review and approval periods, testing and training windows, privacy and security reviews, hardware delivery and setup, go-live readiness, holidays, City closures, known blackout periods, City operational calendars, Program Development Contractor dependencies, and critical path activities.
- **Resource Allocation & Staffing Plan**
Identify key personnel, roles, and qualifications. Describe how resources will be allocated to support project delivery, including any subcontractors.
- **Risk Management & Mitigation**
Identify potential risks to successful implementation and ongoing operations and describe strategies to mitigate those risks.
- **Quality Assurance & Performance Management**
Describe processes for ensuring quality, accuracy, and consistency in service delivery, including performance monitoring and continuous improvement practices.
- **Operational Sustainability**
Explain how the Contractor will support ongoing operations post-implementation, including system maintenance, customer support, and scalability of the solution.
 - Meets requirements 17 to 20 points
 - Meets most requirements 13 to 16 points
 - Meets some requirements 9 to 12 points



- Meets minimal requirements 5 to 8 points
- Meets 1 requirement 1- 4 points
- Does Not Meet requirement 0 points

(4.3) Past Performance 20 points

Past performance of similar projects performed within the last 5 years (State, local, Government, non-profit, volunteer)

- a. Provide a list of a minimum of three (3) prior projects within the last five (5) years in which the firm provided relevant services similar to this assignment. The list shall include the following for each assignment:
 1. Name of client
 2. Location (city and state)
 3. Project/Contract Name
 4. Project Description
 5. Project Duration, which includes the original estimate completion date and the actual completion date
 6. Dollar Amount of Contract
 7. Respondent's scope and role in the project
 1. Provide background information on the project or projects presented to demonstrate expertise
 2. Methodology, tools, and/or processes utilized in performing the work
 3. Demonstration of compliance with any applicable laws, regulations, Executive Orders, OMB Circulars, professional standards, etc.
 4. Project schedule (i.e., major milestones, tasks, deliverables), including an explanation of any delays.
 5. Summary of final deliverables for the noted project or projects.
 8. Client reference for services provided including name, position, phone, and email. All examples of completed services shall have been found to be acceptable by the client. If the Contractor cannot provide three examples of experience, they may provide additional documentation to substantiate project experience to be evaluated by BCIT.
 9. Identify the personnel that will be assigned to the key positions, including subcontractors.
 10. The contractor must provide a minimum of three (3) other government clients at the local, state, or federal levels, non-profit.



11. The contractor must provide referenceable experience delivering three (3) or more similarly sized projects.

- Meets requirements 17 to 20 points
- Meets most requirements 13 to 16 points
- Meets some requirements 9 to 12 points
- Meets minimal requirements 5 to 8 points
- Meets 1 requirement 1- 4 points
- Does Not Meet requirement 0 points

(4.4) Compliance and Security 15 points

The Contractor shall demonstrate its ability to meet all applicable security, privacy, and compliance requirements associated with the implementation and operation of the Municipal Identification Card Program. Proposals must clearly describe the Contractor's approach to safeguarding sensitive data, ensuring system integrity, and maintaining compliance with applicable federal, state, and local regulations.

- Meets requirements 13 to 15 points
- Meets most requirements 10 to 12 points
- Meets some requirements 7 to 9 points
- Meets minimal requirements 4 to 6 points
- Meets 1 requirement 1- 3 points
- Does Not Meet requirement 0 points

The Contractor shall submit a Privacy-by-Design Data Handling Matrix identifying every data element processed by the solution, including but not limited to name, address, date of birth, photo, signature, document type, document image, appointment information, card number, issue date, expiration date, card status, operator ID, audit logs, and reporting data. For each element, the matrix shall state whether the data is captured, printed, stored, transmitted, logged, cached, backed up, exported, or disclosed; the storage location; retention period; deletion method; and whether the data appears in system logs, print queues, browser cache, device storage, analytics tools, backups, vendor support tools, or third-party services. The solution shall not retain prohibited PII beyond the transient processing necessary to complete card issuance.

At a minimum, the Contractor shall address the following:

- **Data Security & Privacy Protections**
Describe how the solution protects personally identifiable information (PII), including



data encryption (in transit and at rest), access controls, user authentication, and data minimization practices.

- **Compliance with Applicable Standards**
Identify and demonstrate compliance with relevant standards and frameworks (e.g., NIST, SOC 2, ISO 27001, ISO/IEC 14443 for the chip interface, WCAG 2.1, as well as any Maryland or City-specific data security requirements).
- **System Security Architecture**
Provide an overview of the system architecture, including hosting environment (e.g., cloud provider), network security controls, and separation of environments (production, test, development).
- **Incident Response & Breach Notification**
Describe the Contractor's incident response plan, including detection, incident severity levels, escalation paths, City notification timelines, containment procedures, forensic support, corrective-action reporting, and post-incident review.
- **Data Ownership, Retention, and Disposal**
Clearly define data ownership, data retention policies, and secure data destruction procedures upon contract termination or at the City's request.
- **Hardware Security (if applicable)**
Describe controls for securing physical devices, including device configuration, access restrictions, tracking, and protection against unauthorized use or tampering.
- **Ongoing Monitoring & Risk Management**
Explain how the system will be monitored for vulnerabilities, including patch management, regular security updates, and third-party assessments or audits.

(4.5) Price 5 points

The Evaluation Committee reserves the right to request Best and Final Offers from all respondents that submit proposals

5. Scope of Work (SOW) and Requirements

5.1 Detailed Specifications:

The City has determined that an integrated, single-vendor solution is necessary to ensure system interoperability, accountability, and streamlined implementation.

The City requires an integrated solution with a single prime Contractor responsible for end-to-end performance of the technology platform, hardware, configuration, interfaces, security, testing, training on technology components, maintenance, and support. The use of subcontractors is permitted only as approved by the City, and the prime Contractor shall remain fully accountable for all subcontractor performance, deliverables, security



obligations, warranties, and service levels. The Contractor shall disclose all subprocessors, hosting providers, support vendors, analytics providers, and third-party service providers used in connection with the solution and shall obtain prior written City approval before adding or replacing such entities. The Contractor shall coordinate with any City-designated Program Development Contractor, but such coordination shall not reduce the Contractor's responsibility for the technology solution.

A. General:

Responsibilities include but are not limited to the design, implementation and maintenance of a system, including supplemental hardware, that provides for:

- (1) Production of physical identification cards with enhanced security features;
- (2) Develop an anonymized online appointment portal that supports scheduling, rescheduling, cancellation, location selection, appointment capacity management, reminders, and reporting without retaining applicant names, addresses, identity documents, or other prohibited PII. If the City elects to collect limited contact information for reminders, the Contractor shall identify the data collected, purpose, retention period, consent language, deletion process, and safeguards, and such collection shall be subject to City approval. The portal should provide the ability for applicants to complete and submit application forms online.
- (3) Products for identity and document authentication in accordance with the industry-standard document authentication and identity verification practices aligned with applicable federal and state guidance (e.g., Hague Convention, NIST Identity Assurance Levels or equivalent frameworks) without making any physical or electronic copies of any documents provided by the applicant as required by the City Code. The solution shall support document authentication and identity verification workflows without retaining originals, copies, scans, photographs, or electronic images of documents presented by applicants. The Contractor shall describe supported document types; authentication methods; hardware or software used; operator workflow; handling of documents that cannot be automatically authenticated; training requirements; false positive/false negative mitigation; audit logging without PII; and how the solution prevents document images or document data from being stored in local device memory, browser cache, print queues, temporary files, system logs, backups, or vendor support systems;
- (4) The solution shall support document verification for all identity document types . Document authentication hardware shall be capable of processing foreign-issued and non-standard document types. The system shall accept documents expired up to five (5) years;
- (5) The enrollment system shall not require information or documentation that would exclude any applicant based on the characteristics enumerated in the City Code;
- (6) Controlled validation of card status shall be provided through a City-approved validation service or secure data exchange. The solution shall support validation of whether a card number is active, expired, lost, stolen, revoked, replaced, or otherwise invalid. The validation process shall not disclose or expose cardholder PII and shall not create a list of



names, addresses, or applicants. Any data exchange shall be limited to permitted non-PII fields, documented in a City-approved interface control document, and protected through access controls, audit logging, and data-use restrictions;

- (7) Hardware for fixed and mobile sites. The Contractor shall provide a fixed-site and mobile-site hardware and operations plan. The plan shall identify the number and type of devices proposed for each issuance model, including printers, cameras, signature pads, document authentication devices, laptops/tablets/workstations, secure card stock storage, network equipment, power needs, transport cases, and spare devices. The plan shall describe setup and teardown time, minimum connectivity requirements, offline or degraded-connectivity procedures, device authentication, inventory tracking, tamper controls, warranty coverage, and replacement service levels; and,
- (8) Multi-lingual and accessible systems for users and ID cardholders.
- (9) The system shall not be used to require individuals to present a Municipal ID Card to access services where government-issued identification was not previously required.

All work and materials must comply with the Baltimore City Code requirement that the City “not retain originals or copies of documents provided by an applicant to prove his or her identity or residency” nor “retain or create lists of the names or addresses of municipal ID card applicants or holders” as well as the Maryland Public Information Act, Maryland’s protection for identifiable information in Subtitle 13 of Title 10 of the State Government Article of the Maryland Code, any applicable federal law as well as BCIT’s web and security standards.

6. DEFINITIONS

For purposes of this Professional Services Request for Proposals (“RFP”) and any resulting Agreement, the following terms shall have the meanings set forth below:

1. **Acceptance Criteria:** Acceptance Criteria means the specific, measurable conditions that a Deliverable must satisfy to be accepted by the City, including requirements related to functionality, performance, completeness, and compliance with the Scope of Work.
2. **Anonymized Data:** Anonymized Data means data that has been irreversibly altered so that an individual cannot be identified by any means reasonably likely to be used, including through data linkage or re-identification techniques
3. **Best Value:** Best Value means the optimal combination of price and non-price factors, as determined by the City in accordance with the evaluation criteria set forth in this RFP.
4. **Card Lifecycle:** Card Lifecycle means all stages of a Municipal ID Card, including application, verification, issuance, activation, renewal, replacement, expiration, and deactivation.
5. **Data Breach:** Data Breach means a confirmed incident in which sensitive data, including Personally Identifiable Information (PII), is accessed, disclosed, or used in an unauthorized manner.
6. **Data Retention:** Data Retention means the storage, maintenance, or preservation of data in any format, including temporary, cached, or backup storage. Data retention does not



include transient processing in system memory where data is not written to persistent storage.

7. **De-Identified Data:** De-Identified Data means data that has been processed to remove or obscure all direct and indirect identifiers such that the data cannot reasonably be used, alone or in combination with other available information, to identify an individual. De-identified data shall not contain combinations of indirect identifiers or quasi-identifiers that could reasonably permit re-identification of an individual when combined with other available information.
8. **Document Authentication:** Document Authentication means the process of assessing the validity of identity or residency documents using industry-standard techniques or tools without retaining copies or images of such documents.
9. **Fraud Prevention System:** Fraud Prevention System means a set of tools, processes, and technologies designed to detect, prevent, and respond to fraudulent applications or misuse of Municipal ID Cards using methods that do not rely on the retention of Personally Identifiable Information.
10. **Identity Verification:** Identity Verification means the process of reviewing applicant-provided documentation to confirm eligibility for a Municipal ID Card, without retaining copies or records of such documentation, in accordance with applicable law.
11. **Incident or Security Incident:** Incident or Security Incident means any actual or suspected unauthorized access, use, disclosure, modification, or destruction of data, or interference with system operations.
12. **Material Deficiency:** Material Deficiency means a defect or failure that significantly impacts system functionality, performance, security, or compliance with the requirements of this RFP or any resulting Agreement.
13. **Metadata:** Metadata means operational, transactional, technical, or system-generated information associated with user activity, including but not limited to IP addresses, timestamps, session identifiers, browser telemetry, device identifiers, geolocation information, access logs, usage analytics, API activity, and audit records.
14. **Municipal ID Card:** Municipal ID Card means a City-issued identification credential under Baltimore City Code Subtitle 38 that includes limited personal information displayed on the physical card but is not supported by a backend system that retains identifying information about the cardholder.
15. **No Data Retention Requirement:** No Data Retention Requirement means that the solution shall not store, archive, maintain, log, cache, back up, export, or otherwise preserve prohibited Personally Identifiable Information (PII) beyond the time necessary to complete real-time identity verification and card issuance. This prohibition includes originals or copies of applicant identity or residency documents and lists of applicant or cardholder names or addresses. Any such data must be immediately discarded and not recoverable after completion of the transaction.



16. **Notice to Proceed or “NTP”:** Notice to Proceed or “NTP” means the formal written authorization issued by the security requirements City allowing the Contractor to begin performance under the Agreement.
17. **Personally Identifiable Information or “PII”:** “Personally Identifiable Information” or “PII” means any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information, including but not limited to name, address, date of birth, identification numbers, photographs, or any other data that could reasonably be used to identify an individual. PII includes metadata where such metadata could reasonably be used to identify, profile, locate, track, or reconstruct activity of an individual.
18. **Responsive Proposal:** Responsive Proposal means a proposal that conforms in all material respect to the requirements of this RFP.
19. **Responsible Contractor:** Responsible Contractor means a Contractor that possesses the capability, integrity, and reliability to fully perform the requirements of this RFP and any resulting Agreement.
20. **Role-Based Access Control or “RBAC”:** Role-Based Access Control or “RBAC” means a system of restricting system access based on user roles and responsibilities, ensuring that users can only access information necessary to perform their assigned duties.
21. **Service Level Agreement or “SLA”:** Service Level Agreement or “SLA” means the measurable performance standards agreed upon by the City and the Contractor, including but not limited to system availability, response times, resolution times, and support requirements.
22. **System Availability or “Uptime”:** System Availability or “Uptime” means the percentage of time that the system is fully operational and accessible to authorized users, excluding scheduled maintenance periods approved by the City.
23. **Tokenized Data:** Tokenized Data means sensitive data elements that have been replaced with non-sensitive equivalents (tokens) that have no exploitable meaning or value and cannot be reverse-engineered without access to a secure tokenization system.
24. **Material Deficiency:** Material Deficiency means any defect, omission, error, or nonconformance that materially impacts the functionality, security, performance, compliance, or intended use of a Deliverable, including failure to meet the requirements, specifications, or Acceptance Criteria set forth in this RFP or resulting Agreement. A Deliverable shall be considered to have no material deficiencies when it performs in accordance with all required functionality, meets defined Acceptance Criteria, and does not contain any defects that would impair the City’s ability to use the Deliverable for its intended purpose.cc

In the event of any ambiguity, inconsistency, or conflict between requirements set forth in this professional services RFP, the City reserves the right to interpret such requirements in a manner that best aligns with applicable law, program objectives, and operational needs. Contractors are



responsible for identifying and clearly stating any assumptions made in the preparation of their proposals.

7. DETAILED SCOPE OF WORK:

The end product will encompass all aspects of the development and implementation of the Program.

BCIT's requirements for the Program include the following:

A. PROGRAM DEVELOPMENT AND DESIGN

1. The Contractor shall advise on the design of specified elements of the Program including:
 - Intake materials (forms and instructions);
 - Scoring or point system to evaluate proof of identity and residency documents provided by municipal ID card applicants consistent with the City Code;
 - Process development for ID life cycle including renewal, expiration, card replacement (e.g. for lost or stolen cards) and change of address services; and,
 - A programmatic and/or technological system to detect and prevent fraudulent use of the municipal identification cards. This system may NOT retain descriptive or demographic data tied to a particular ID municipal identification card. The card may contain electronic or other guarantees of being an authentic card.

B. CARD DESIGN AND PRODUCTION

2. The solution shall support the full Municipal ID card lifecycle, including application intake, eligibility verification, card production, activation, issuance, renewal, replacement, expiration, deactivation, lost/stolen reporting, damaged-card replacement, surrendered-card processing, and status updates. The Contractor shall describe proposed status values and allowed status transitions. The solution shall support duplicate-prevention and fraud-prevention approaches that do not require the retention of prohibited PII. The solution shall maintain only City-approved non-PII lifecycle data, such as card number, issue date, expiration date, status, termination/deactivation date, and operator/system audit information.

The Contractor shall propose a card design and production approach that includes: card dimensions and material; card durability; front/back layout; required and optional printed fields; city seal/logo placement; unique card number; issue and expiration dates; barcode, magnetic stripe, RFID, or other technology if proposed; anti-counterfeit features; and a card stock inventory control process. Required card-security features shall include, at minimum, tamper-resistant card material, unique card/card-stock number, high-quality photo, expiration date, city branding/seal, and at least two visual or tactile anti-counterfeit features. The Contractor shall



clearly identify which features are included as standard and which are optional or separately priced.

The Contractor shall design and produce a secure, tamper-proof identification card that meets the following standards:

- Cost effective, efficient, sustainable, and designed to prevent fraud and misuse;
- Enhanced card security utilizing features such as laser-engraved serial numbers on card stock, fine-line pattern backgrounds, embedded watermarks, ultraviolet ink, holograms, tamper-evident magnetic stripes, and tamper-proof signature panels;
- Included Level 1 Homeland Security features for national and state identification cards;
- Consistent with the bank's Customer Identification Program Requirements under Section 326 of the USA PATRIOT ACT to ensure that the card align with commonly accepted identity verification standards to support potential acceptance as a primary proof of identity and/or residence by financial institutions if that is possible given the requirement that there can be no retention of records of names or identifying information for the individuals holding municipal ID cards as required by the City Code;
- Complies with federal identification and anti-money laundering standards to allow for use at financial institutions as specified by the Federal Reserve, the U.S. Treasury Department, and the Office of the Comptroller of the Currency if that is possible given the requirement that there can be no retention of records of names or identifying information for the individuals holding municipal ID cards as required by the City Code;
- Include demographic information on card such as unique ID numbers, full legal names, date of birth, expiration date, and photograph, in accordance with local law. The card shall not display the cardholder's gender,
- Ensures visual accessibility for residents with disabilities (e.g., high contrast, readable fonts); and,
- Allows layering other city services on the base card such as municipal library or recreation and parks card barcodes.

C: HARDWARE

3. The Contractor shall provide all required hardware for card production and application processing at both fixed and mobile sites including:
 - Hardware for a permanent site and/or mobile workstations, including all equipment necessary to implement designed system (e.g. cameras, back drop, scanners, printers);
 - Printing ribbons must not retain personally identifiable information;
 - Fixed-location and mobile workstations contain separate dedicated printers;



- Fixed-location workstations must also have the capacity to be mobilized for setup at an off-site location;
Verification hardware using secure document and data authentication;
- Adequate testing of systems to detect and mitigate risks, detect and cure defects, and prevent system failures;
- Maintenance and support for all hardware for the duration of the contract; and launch and consumables (ribbons, card stock) for at least 8,000 ID cards in Year 1 of the program; and, training for administrators and card processors detailing safe and effective use of products provided.

The Contractor shall describe controls for preventing, clearing, securing, or destroying any such artifacts. Any technology that retains readable PII on spent ribbons, transfer media, printer memory, or other physical or digital artifacts must include a City-approved secure handling and destruction process, and may be rejected if inconsistent with City privacy requirements.

D. SOFTWARE

4. The Contractor shall develop and configure SaaS platforms tailored to the Program's needs such as:
 - Develop a public, anonymized online appointment portal that meets state and federal accessibility guidelines and includes the ability for applicants to complete and submit application forms online;
 - User-friendly system for entering photo, name, date of birth, unique municipal ID card number, and expiration date to be printed on ID cards, with no data storage or retention;
 - The system shall track municipal ID card numbers, issuance dates, expiration dates, and de-identified demographic data as specified by BCIT. The system shall not retain personally identifiable information (PII) that can be used to identify an individual. The system may retain anonymized, de-identified, or tokenized data for operational, reporting, fraud prevention, and audit purposes, provided that such data cannot reasonably be used to re-identify any individual;
 - Compatibility with the City's infrastructure, including secure cloud-based hosting environments such as Azure Government Cloud;
 - Role-based access control and data protection to safeguard sensitive data and ensure compliance with state, federal, and City standards;
 - Maintenance and support of software provided and/or managed by Contractor;
 - Public facing training and materials related to appointment portal navigation;
 - Accessible features for limited English proficient residents in compliance with federal and local regulations; The solution shall meet applicable accessibility requirements, including WCAG 2.1 AA or the City-approved equivalent for public-facing and staff-facing digital components. The Contractor shall describe



language capabilities for applicant-facing workflows, appointment communications, instructions, error messages, training materials, and support content. The solution shall support City-approved language access requirements and shall allow the City to update translated content without vendor code changes where feasible; and,

- Regular updates software updates, patches, and security enhancements to address vulnerabilities and improve functionality.
- The solution shall support configurable program rules and parameters to accommodate administrative rules and regulations adopted by BCIT, without requiring custom code changes.
- The solution shall support configurable application fees as set by the Board of Estimates including full and partial fee waiver processing. Fee amounts, waiver eligibility criteria, and payment methods shall be configurable by City administrators without custom code changes.
- The platform shall support a homeless residency verification pathway including acceptance of shelter-recognized identity documents and alternative address handling for applicants without a fixed residential address (e.g., shelter address, care-of address).

E. TESTING, ACCEPTANCE, AND GO-LIVE READINESS

- Develop and execute a City-approved test strategy covering configuration testing, device integration testing, card print-quality testing, document authentication workflow testing, no-retention/privacy testing, API/interface testing, accessibility testing, mobile-site connectivity testing, performance/load testing, security testing, disaster recovery testing, user acceptance testing, and operational readiness testing. Provide test scripts, expected results, evidence of execution, defect logs, severity levels, remediation plans, retest results, and a go-live readiness checklist. Correct all critical and high-severity defects identified during testing prior to production launch, unless the City provides written approval for a documented workaround or deferred remediation plan.

No production launch shall occur until the City provides written acceptance.

F. TECHNOLOGY TRAINING PLAN AND KNOWLEDGE TRANSFER

- The Contractor shall provide a Technology Training Plan for City review and approval. The plan shall describe the training approach, target audiences, curriculum, delivery methods, schedule, training materials, trainer qualifications, attendance tracking, knowledge-transfer approach, and post-training support.
- At a minimum, the Contractor shall provide technology training for City staff, system administrators, support personnel, and approved partners who will use, maintain, administer, or support the solution. Training shall include, as applicable, system administration, enrollment workflow, identity verification workflow, document authentication workflow, card production and printing, hardware operation, mobile-site



setup, troubleshooting, privacy and no-retention procedures, role-based access, reporting, API or card-validation processes, incident reporting, and support escalation procedures.

- The Contractor shall provide role-based training materials, user guides, job aids, quick reference guides, and train-the-trainer materials. The Contractor shall also provide refresher training or updated materials when material system changes, workflow changes, or new functionality is introduced during the contract term.
- Broader public education, community outreach, program-policy training, and partner adoption strategy shall be coordinated with the City and any separately procured Program Development Contractor. The Contractor shall coordinate with the City and any Program Development Contractor to ensure technology training materials reflect approved program policies, operating procedures, privacy requirements, and user roles.

G: CONFIDENTIALITY

G.1 The City is committed to protecting the privacy of all Program participants. The Contractor shall ensure that all solution components, workflows, devices, integrations, reports, logs, support tools, and vendor-managed environments comply with Baltimore City Code and all applicable confidentiality, privacy, and data-retention restrictions:

- No originals or copies of identification documents will be retained by the City, the Contractor, or any subcontractor.
- The solution shall not retain the names of municipal identification card applicants or holders.
- No personally identifiable information reviewed, including but not limited to cardholder names and addresses, identification numbers, as well as documents proving identity, will be retained. The solution shall not retain prohibited personally identifiable information beyond the transient processing necessary to complete identity verification and card issuance. Any prohibited personally identifiable information used transiently during issuance must be immediately discarded and not recoverable after completion or cancellation of the transaction.
- Original documents must not be retained and may only be reviewed to verify their information by the by the Contractor.
- The solution shall not store, archive, maintain, log, cache, back up, export, or otherwise preserve prohibited personally identifiable information in databases, local device storage, browser cache, print queues, printer memory, temporary files, application logs, audit logs, analytics systems, backups, support tools, monitoring tools, third-party services, or vendor-managed environments.
- The Contractor shall describe the technical, procedural, and operational controls used to prevent prohibited data retention, including controls for devices, printers, print ribbons, cameras, document authentication tools, browser sessions, logs, backups, support access, and third-party services.



- The Contractor shall develop Staff and partner procedures governing the use of Municipal ID systems and processes ensuring cardholder privacy, data integrity and the City's privacy and no-retention requirements.
- Documents should not be retained as no records can be kept pursuant to Section 38-10 of Article 1 of the City Code; and,
- The Contractor shall comply with the City's IT Security Rider and all applicable City security, privacy, accessibility, and data-protection requirements. The Contractor and all subcontractors, subprocessors, hosting providers, and affiliated entities shall not use, disclose, analyze, monetize, benchmark, mine, aggregate, train artificial intelligence systems on, or otherwise process Program data, metadata, or operational information for any purpose other than direct performance of this Agreement.

G.2 The Contractor shall not disclose Program-related data, metadata, logs, operational records, audit information, or system information to any third party, including law enforcement or federal agencies, absent prior written authorization from the City unless legally prohibited from doing so.

The Contractor shall notify the City immediately upon receipt of any subpoena, warrant, court order, preservation request, administrative request, or other inquiry seeking access to Program-related information.

Where legally permissible, the Contractor shall cooperate with the City in challenging, narrowing, or limiting such requests.

The Contractor shall maintain written procedures governing responses to law enforcement and government requests related to the Program.

G.3 Public Statements and Marketing. The Contractor shall not issue press releases, public statements, case studies, conference presentations, marketing materials, or promotional content referencing the Program or the City without prior written approval from the City.

H: MONITORING AND REPORTING

H.1 The Contractor shall implement a reporting system that includes:

- Exportable data formats such as .csv or similar;
- Custom dashboards for ongoing program monitoring and evaluation which may include, but is not limited to, the following:
 - Detailed project management updates and progress reports;
 - Average customer wait time;
 - Average customer processing time;
 - Application approval rate;
 - Customer satisfaction metrics;



- Number of Municipal ID cards issued;
- Customer service survey reports summaries; and
- Other performance measures or items as requested by the City.

H.2 Privacy-Safe Reporting and Analytics

All reporting, dashboards, analytics, and operational metrics shall use aggregate, anonymized, or de-identified data only and shall be designed to prevent re-identification of applicants or cardholders, including through small-cell reporting, linkage with other datasets, or inference from location, time, demographic, appointment, or issuance data. The Contractor shall not use City data for product analytics, model training, marketing, benchmarking, or any purpose not expressly approved by the City.

Program data, metadata, logs, operational records, or validation activity shall not be shared with commercial data brokers, identity networks, investigative databases, marketing databases, or third-party aggregation services.

Technology Training Requirements

The Contractor shall develop and provide a comprehensive Technology Training Plan to support successful implementation and use of all systems, software, and hardware delivered under this Agreement.

At a minimum, the Contractor shall submit a written narrative describing the proposed training program, which shall include:

1. Course Names – A list of all training courses to be provided;
2. Course Descriptions – A brief description of each course, including learning objectives and intended audience;
3. Duration – The length of each training session (e.g., hours or days);
4. Training Type – The format of training (e.g., in-person, virtual, hybrid, instructor-led, self-paced);
5. Training Location – Identification of where training will occur (on-site, off-site, or virtual); and
6. Additional Details – Any other relevant information, including required materials, prerequisites, number of participants supported, and post-training support or resources.

The Contractor shall ensure that all training is aligned with the functionality and operational requirements of the Solution and is sufficient to enable City staff and designated users to effectively operate and maintain the system.

Authorization Requirement: If the Contractor is not the original equipment manufacturer (OEM) or software provider, the Contractor shall provide documentation demonstrating authorization to deliver training on the applicable software and/or hardware products.



I: OUTREACH

G.1 The Contractor shall support outreach and engagement activities necessary for successful implementation and use of the solution. This may include system demonstrations, training sessions and public engagement activities as needed, including but not limited to:

- Assisting with FAQs, user guidance, responses to questions related to the products, tools, workflows, and services provided by the Contractor ~~received from the public, elected officials, or media on all products provided~~; and
- Participating in focus groups, supported by community advocates, to understand how different communities use identification and to identify accessibility challenges.

J. SERVICE LEVELS, MAINTENANCE, AND SUPPORT

The Contractor shall provide proposed service levels at or above the following minimums: SaaS availability of 99.9% monthly excluding City-approved maintenance; critical incident response within 1 hour; critical incident workaround or resolution target within 4 to 8 hours; high-severity incident response within 4 business hours; scheduled maintenance notice at least 7 calendar days in advance; emergency maintenance notice as soon as practicable; critical security patching within 7 days; high security patching within 30 days; hardware replacement or functional workaround by next business day for card-production-blocking failures; and disaster recovery objectives including proposed Recovery Time Objective and Recovery Point Objective for permitted data.

In the event of ambiguity or conflict between requirements, the City reserves the right to clarify intent through written addenda. Contractors are responsible for identifying assumptions in their proposals. The City will evaluate proposals based on reasonable interpretations aligned with the Program's objectives.



#	Deliverable Name	Description / Scope	Format / Acceptance Criteria	Due Date / Milestone	City Review & Approval	Payment Milestone
1	Workplan	Authoritative roadmap detailing configuration, deployment, transition to operations and an integrated City-Contractor project schedule.	Written work that includes project phases milestones, Contractor activities, City activities, roles and responsibilities, dependencies, decision points, City inputs and approvals, training schedule, OCM and readiness activities, adoption support, implementation timeline, and an integrated City-Contractor project schedule. The schedule must account for City operational calendars, resource availability, review and approval cycles, Program Development Contractor dependencies, and other constraints that may affect the implementation timeline. The workplan shall be reviewed with the City on a recurring cadence and updated as assumptions, dependencies, or constraints change. Approved by the City Project Manager; workplan submitted in complete form; usable for project execution and contains no material deficiencies.	Within 10 business days of Notice to Proceed (NTP)	BCIT Project Manager	Included in initial invoice



2	Process Design Materials	Intake materials, ID card lifecycle design materials, and program design for fraud prevention program.	Written work approved by the City Project Manager; work completed, no material deficiencies.	Within 30 business days of NTP	BCIT Project Manager	Milestone-based payment
3	Printing related hardware for stationary and mobile sites	Hardware to capture applicant data, produce physical IDs with fraud deterrence features, and encode ID if necessary and instructions and/or training for effective use.	Hardware including but not limited to workstation printers, scanners, signature pads, backdrops as agreed upon in contract and approved by the City Project Manager; materials provided, no material deficiencies, ongoing support if needed.	60 days after NTP	BCIT Project Manager	Milestone-based payment
4	Appointment Portal	Self-scheduled time slots for ID enrollment which allows for rescheduling or cancellation.	Complete operational system with administrative credentials owned by City and approved by the City Project Manager; no material deficiencies. Ongoing patching if needed.	As scheduled in approved Work Plan	BCIT Project Manager	Included in progress invoice
5	ID Management Software	Data entry application which is able to process application information, catalogue IDs issued and expiration dates, store de-identified data, and track program metrics.	Complete operational system with administrative credentials owned by City and approved by the City Project Manager; no material deficiencies. Ongoing patching if needed.	As scheduled in approved Work Plan	BCIT Project Manager	Included in progress invoice
6	Verification related hardware and software for stationary and mobile sites	Verification hardware and/or software that can review, validate, and document applicant eligibility prior to ID issuance. Additional hardware,	Complete operational system with administrative credentials owned by City and approved by the City Project Manager; no material deficiencies. No ability	As specified in approved Work Plan	BCIT Project Manager	Milestone-based payment

		if needed, for fraud detection program.	to retain information of documents provided.			
7	Testing, Acceptance, and Go-Live Readiness Package	City-approved test strategy, test scripts, test evidence, defect log, remediation plan, retest results, privacy/no-retention test results, security test results, accessibility test results, operational readiness checklist, and go-live recommendation.	Written testing package approved by the City. Acceptance requires completion of required testing, no open critical or high-severity defects unless expressly approved by the City in writing, successful no-retention/privacy testing, successful card-production testing, successful validation/API testing if applicable, successful independent third-party penetration test with all critical and high severity findings remediated, and written City approval to proceed to production launch.	As specified in approved Work Plan	BCIT Project Manager and City technical/security reviewers.	Required before production/go-live payment.
8	Progress Dashboard	Reporting system that includes exportable data formats such as .csv or similar for ongoing program monitoring and evaluation .	Complete operational system with administrative credentials owned by City and approved by the City Project Manager; no material deficiencies, no ability to retain information of documents provided.	As specified in approved Work Plan	BCIT Project Manager	Included in progress invoice
9	Technology Training Plan and Knowledge Transfer Package	Technology Training Plan, public engagement activities, role-based curriculum, user guides, job aids, quick reference guides, system administrator materials, train-the-trainer package, attendance	City-approved training plan and materials; completion of required training sessions for City staff, administrators, support personnel, and approved partners; submission of final accepted	Initial Training Plan due within sixty (60) days after NTP. Final training and	BCIT Project Manager with review by the City Organizational Change Manager	Milestone-based payment



		tracking, and knowledge-transfer materials.	training materials; no material deficiencies..	engagement materials due as specified in the approved Work Plan.		
10	Privacy and No-Retention Controls Plan	Written plan describing the technical, procedural, and operational controls used to prevent prohibited data retention across all solution components, including devices, printers, print ribbons, cameras, document authentication tools, browser sessions, logs, backups, support access, third-party services, and vendor-managed environments.	City-approved written plan that identifies each control, the system component or workflow it applies to, how the control prevents retention of prohibited data, how compliance will be tested or validated, and any Contractor, subcontractor, or City responsibilities. The plan must demonstrate compliance with Baltimore City Code and contain no material deficiencies.	Prior to configuration completion and before system testing begins, or as specified in the approved Work Plan.	BCIT Project Manager, with review by City technical/security reviewers as applicable	Required before testing/go-live readiness payment.

No Data Retention Requirement means the solution shall not store, archive, maintain, log, cache, back up, export, or otherwise preserve prohibited PII beyond the transient processing necessary to complete real-time identity verification and card issuance. This prohibition includes databases, local device storage, browser cache, print queues, printer memory, temporary files, application logs, audit logs, analytics systems, backups, support tools, monitoring tools, third-party services, and vendor-managed environments. Any prohibited PII used transiently during issuance must be immediately discarded and not recoverable after completion or cancellation of the transaction.



4. Security Requirements

DEFINITIONS

For purposes of the Agreement:

(1) “Sensitive data” means information that is protected against unwarranted disclosure, to include Personally Identifiable Information (PII), Protected Health Information (PHI), Criminal Justice Information (CJI), Payment Card Industry (PCI) data, or any other private/confidential data as determined by the City, State, or Federal governments. It includes any personally identifiable information contained in any document reviewed by the City or the Vendor prior to returning it to the applicant.

(2) “Relevant subcontractor” includes any subcontractor that assists the Contractor in the critical functions of the Agreement, handles sensitive data, and/or assists with any related implemented system, excluding subcontractors that provide secondary services that are not pertinent to assisting the Contractor in the critical functions of the Agreement, handling sensitive data, and/or assisting with any related implemented system.

DATA OWNERSHIP

The City solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all City’s data. The Contractor has no and acquires no right, title or interest, whether express or implied, in and to City’s data. The Contractor will only use City’s data for the purposes set forth in the Contract. The Contractor will only access City’s data as necessary for performance of the Agreement. The Contractor will not access City’s user accounts except to respond to service or technical problems or at the City’s specific request. All City’s data, including copies, summaries and derivative works thereof, must be remitted, in a mutually agreeable format and media, to the City by the Contractor upon request or upon completion, termination or cancellation of the Contract. The foregoing sentence does not apply if the City’s Chief Information Security Officer or delegate authorizes in writing the Contractor to sanitize and/or destroy the data and the Contractor certifies in writing the sanitization and/or destruction of the data.

In the event of loss of any City’s data or records where such loss is due to the intentional act or omission or negligence of the Contractor or any of its subcontractors or agents, the Contractor shall be responsible for recreating such lost data in the manner and on the schedule set by the City. The Contractor shall ensure that all data is backed up and recoverable by the Contractor. The Contractor shall use its best efforts to assure that at no time shall any actions undertaken



by the Contractor under this Agreement (or any failures to act when Contractor has a duty to act) damage or create any vulnerabilities in data bases, systems, platforms, and/or applications with which the Contractor is working hereunder.

INFORMATION SECURITY REQUIREMENTS

The Contractor, including any relevant subcontractor(s), shall implement administrative, physical, and technical safeguards to protect City's data that are no less rigorous than accepted industry standards for information security such as those listed below, and ensure that all such safeguards, including the manner in which City's data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of this solicitation and resulting Agreement.

To ensure appropriate data protection safeguards are in place, the Contractor and any authorized relevant subcontractor(s), who would be handling City's sensitive data or interconnect to City's computerized systems, shall at a minimum implement and maintain the following information technology controls at all times throughout the life of the Agreement. The Contractor and any authorized relevant subcontractor(s) may augment this list with additional information technology controls.

(1) Agrees to abide by all applicable federal, State and local laws and standards concerning information security and shall comply with all such revisions.

Yes

No (add comment below)

(2) Conduct basic security awareness training on regular bases, for all Contractor /subcontractor personnel.

(3) Establish separate production, test, and development environments for systems supporting the services provided under this Agreement and ensure that production data is not replicated in the test and/or training environment unless it has been previously anonymized or otherwise modified to protect the confidentiality of sensitive data elements.

(4) Apply hardware and software hardening procedures as recommended by the manufacturer to reduce the Contractor /subcontractor's systems' surface of vulnerability. The purpose of system hardening procedures is to eliminate as many security risks as possible. These procedures may include but are not limited to removal of unnecessary software, disabling or removing of unnecessary services, removal of unnecessary usernames or logins, and deactivation of unneeded features in the Contractor /subcontractor's system configuration files.



(5) Develop and implement a local patching policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes on the Contractor /subcontractor's systems. The purpose of regular software patches is to eliminate as many software vulnerabilities as possible remediating critical and high vulnerabilities within 30 days.

(6) The City may require the Contractor provides the City notice in writing of all scheduled or automatic updates. The updates or Software maintenance shall include, but not limited to: cover bugs that did not show during original testing and de-bugging; improvements and enhancements to the Software; patches; new versions of the Software; users discover new ways to make an error; Software environment changes (i.e., new operating system); hardware environment changes; user requirement changes; and communication environment changes (i.e., LAN, internet use).

(7) Establish policies and procedures to implement and maintain mechanisms for regular internal vulnerability testing of operating system, application, and network devices supporting the services provided under this Agreement. Such testing is intended to identify outdated software versions; missing software patches; and device or software misconfigurations; and validate compliance with or deviations from the Contractor's and/or subcontractor's security policy.

The Contractor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The City shall have the right to inspect these policies and procedures.

(8) Where website hosting or Internet access is the service provided or part of the service provided, the Contractor and any relevant subcontractor(s) shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the

Contractor's and subcontractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The Contractor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The City shall have the right to inspect these policies and procedures.



(9) Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Agreement, automatically updated, and configured to actively scan and detect threats to the system for remediation.

(10) Enforce strong user authentication and password controls, including multifactor authentication, over the Contractor /subcontractor's systems supporting the services provided under this Contract to minimize the opportunity for unauthorized system access through compromise of the user access controls. Where feasible, integrate with City's single sign-on (SSO) system for authentications and authorization of end-users to the provided service.

(11) Ensure City's data under this service is not processed, transferred, or stored outside of the United States.

(12) Ensure that City's data is not comingled with the Contractor's and subcontractor's other clients' data through the proper application of data compartmentalization security measures. This includes but is not limited to classifying data elements and controlling access to those elements based on the classification and the user's access or security level.

(13) Apply data encryption to protect City's data, especially sensitive data, from improper disclosure or alteration. Encryption should be applied to data in transit over networks, at rest within the system, and when archived for backup purposes.

(14) Enable appropriate logging parameters on systems supporting services provided under this Agreement to monitor user activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers as well as information security standards.

(15) Retain the aforementioned logs and manual or programmatically review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and perform remediation, if required. This requirement can be fulfilled by a security information and event management (SIEM) or other similar security analytics platforms.

(16) Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of sensitive data from unauthorized access as well as the separation of production and non-production environments.



(17) Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the services being provided under the Agreement from unsolicited and unauthenticated network traffic.

(18) Review at regular intervals, at least annually, the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.

(19) Ensure that the Contractor's and any subcontractor's personnel shall not connect any of their own equipment to a City's network without prior written approval by the City's IT Department.

(20) Remote access requested by the Contractor to the City's network or systems shall use City's approved remote access solutions

(21) Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate authorities.

(22) The Contractor must provide and maintain a Problem Escalation Procedure (PEP) for both routine and emergency situations.

(23) If Contractor /subcontractor will be storing or processing City's sensitive data they shall make available, prior to agreement start, for City's review results for any independent audit, such as: SOC 2 Security (Common Criteria), ISO 27001, and other relevant audit results.

DATA BREACH NOTIFICATION REQUIREMENTS

(1) If a breach of security or confidentiality occurs that require notice to the City's employees and/or third parties under federal, state or local laws then the City shall have sole control over the timing, content, and method of notice; and the Contractor cannot notify affected individuals unless the City directs the Contractor in writing. The Contractor shall be liable and reimburse the City for its out-of-pocket costs and expenses incurred in giving notice of any security breach for which the Contractor is partially or fully responsible, even if notice is not legally required.



(2) The Contractor shall notify the City (infosec@baltimorecity.gov) when the Contractor and/or any authorized subcontractor system that may access, process, or store City's data or work product is subject to unauthorized access or system compromise. Unauthorized access or system compromise may include compromise by computer malware, malicious search engine, credential compromise, access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

- a. The Contractor shall notify the City within two (2) business days of the discovery of the unauthorized access or system compromise.
- b. The Contractor shall notify the City within twenty-four (24) hours if there was a data breach of the City's sensitive data.

(3) If an unauthorized use or disclosure of any City's sensitive data occurs, the Contractor must provide written notice to the City (infosec@baltimorecity.gov) within twenty-four (24) hours after the Contractor's discovery of such use or disclosure and, thereafter, all information the City requests concerning such unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the City. The Contractor's report shall identify:

- a. Nature of the unauthorized use or disclosure.
- b. Sensitive data used or disclosed.
- c. Who made the unauthorized use or received the unauthorized disclosure.
- d. What the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
- e. What corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

CONTINGENCY / DISASTER RECOVERY PLANS

(1) The Contractor and any authorized relevant subcontractor(s) shall have robust contingency and disaster recovery plans in place to ensure that the services provided under this Agreement will be maintained in the event of disruption to the Contractor /subcontractor's operations (including, but not limited to, disruption to information technology systems), however caused.

(2) The contingency and disaster recovery plans must be designed to ensure that services under this Agreement are restored after a disruption within (specify the time duration in



hours or days in which services must be restored) in order to avoid unacceptable consequences due to the unavailability of services.

(3) Such contingency and disaster recovery plans shall be available for the City to inspect at any reasonable time, and subject to regular updating, revising, and testing throughout the term of the Agreement.

END OF CONTRACT TRANSITION

(1) The Contractor shall cooperate in the orderly transition of services from the Agreement to any subsequent contract for similar services. The transition period shall begin ninety (90) days (or a different number of days, at the City's discretion) before the Agreement end date, or the end date of any final exercised option or contract extension. The Contractor shall work toward a prompt and timely transition, proceeding in accordance with the directions of the City. The City may provide the Contractor with additional instructions to meet specific transition requirements prior to the end of Contract.

(2) Within sixty (60) days after the effective date of termination or expiration of this Agreement or upon the City's request, for any reason, the Contractor shall either scrub, return, or destroy, as directed by the City, all City's data provided to the Contractor by the City, including all City's data provided to, or in the possession of, the Contractor's employees, subcontractors, agents, or other affiliated persons or entities. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

(3) In the event that returning or destroying the City's data is not feasible, the Contractor shall provide notification of the conditions that make return or destruction not feasible, in which case, the Contractor must continue to protect all City's data that it retains, and the Contractor agrees to prevent further uses and disclosures of such data given the return or destruction of the data is not feasible as the Contractor maintains such data.

(4) Upon request by the City made or within thirty (30) days after the effective date of termination or expiration of this Agreement, the Contractor will make available to the City for a complete and secure (i.e. encrypted and appropriately authenticated) download file of City's data including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. The Contractor will be available sixty (60) days after providing the City's data to answer questions about data schema, transformations, and other elements required to fully understand and



utilize the City's data file. After such sixty (60) day period, the Contractor, its hosted service provider, and relevant subcontractors shall have no obligation to maintain or provide any City's data and shall thereafter, unless legally prohibited, delete in such a manner as prevents recovery through normal/laboratory means, all City's data in its systems or otherwise in its possession or under its control. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

(5) It is not just City's data that needs to be returned once this agreement has expired or is terminated. The City might hold confidential information belonging to the Contractor. Accordingly, all confidential information of each party should be returned (or destroyed) and confirmation of destruction of such confidential data (as applicable) must be in writing.

(6) The Contractor acknowledges that it provides services that are critical to the City's business and operations. If the Contractor fails to meet the service levels described in this document, the City may terminate its entire contract with the Contractor, with no penalty.

(7) If the City terminates this Agreement, it may be moving to a competitor. Often the City will need assistance in transferring its data from the Contractor's system to the competitor's system. Any such assistance should only be provided in return for mutually agreed upon payment for such additional services, as such assistance could be substantial and time consuming. However, the City shall not pay for such assistance when it terminates the Contractor for default as such assistance will be at the Contractor's sole cost and expense.



Proposal Response Instructions

1. Proposal Organization and Submission Requirements

Contractors shall submit **one (1) complete proposal volume**, organized into the sections identified below. Each section must be clearly labeled and separated using tabs or dividers to facilitate efficient review and evaluation.

The proposal shall be structured to correspond directly with the scope of work requirements and evaluation criteria set forth in this solicitation. Contractors shall follow the order and headings provided to ensure clarity, completeness, and consistency in evaluation.

At a minimum, the proposal must include responses to the following sections:

- I. Cover Letter** (1 page Maximum)
- II. Table of Contents** (1 page Maximum)
- III. Technical & Implementation Approach** (10 page Maximum)
- IV. Management Approach** (5 page Maximum)
- V. Compliance and Security** (3 page Maximum)
- VI. Past Performance** (2 page Maximum per performance)
- VII. Cost Proposal** (submitted as a separate attachment – 3 page Maximum)

Cover Letter (1 Page Maximum)

The professional services proposal shall be submitted with a cover letter. The cover letter shall provide:

- a. Company Name, Address
- b. Name, Title, Telephone Number, Email Address, for individual authorized to represent the company
- c. Contractors are to clearly detail any exceptions taken and the rationale for the exceptions taken to the Statement of Work. Please note that exceptions taken to the Scope of Work may render the proposal submission unacceptable to the City of Baltimore.
- d. Contractor shall describe any assumptions used to develop the proposal if needed.

1. Executive Summary

- a. Provide a brief history of the firm, including name of the firm, general services, experience, the year the firm was established under the current name, the principal place of business, and the location of local office(s).



- b. Indicate any other previous names of the firm during the last five (5) years and the year any name change was effective. The contractor must have been in operation for a minimum of five (5) years and operating under the same ownership for a minimum of three (3) years.

Paper, Page Size, and Markings: Proposals shall be formatted such that, if printed, they fit within 8 1/2 X 11-inch paper, in a commercially standard font size (no smaller than 11 point). Margins shall be 1 inch at the top, sides and bottom. The Contractor should mark its proposal with any proprietary marking, if needed, based on their assessment of the contents of each proposal.

Illustrations and Tables: Tables, charts, graphs, diagrams, and figures shall be used wherever practical. Illustrations shall be legible. Text shall be no smaller than 10 point font for tables, charts, graphs, and figures.

Contractors shall provide clear, complete, and detailed responses within each section. Failure to include required sections or adequately address the evaluation criteria may result in the proposal being deemed non-responsive or receiving a lower evaluation score.

Web and Mobile Accessibility Compliance: The City, a municipal corporation, is required by Title II of the Americans with Disabilities Act and its implementing regulations at 28 CFR 35 part 35, subpart H (the “Accessibility Rule”) to ensure that all Web Content and Mobile Applications, as defined in 28 CFR 35.104, are readily accessible to and usable by individuals with disabilities. As of the effective date of this Agreement, the Accessibility Rule adopts Web and Mobile Accessibility Compliance (“WCAG”) version 2.1 and requires compliance with WCAG 2.1 success criteria levels A and AA no later than April 24, 2026.

The Contractor shall cause any and all Web Content and Mobile Applications provided under, used to perform, or required for end-user interaction with the Agreement to comply with WCAG 2.1 Level AA or higher, as demonstrated using the Information Technology Industry Council’s Voluntary Product Accessibility Template VPAT version 2.5 WCAG (November 2023), an updated VPAT designed for enforcement of the Accessibility Rule, or a similar compliance tool if specified by the City, no later than April 24, 2026 and for the term of the Agreement.

The Contractor shall continue to ensure its Web Content and Mobile Applications provided under the Agreement comply with the then-current version of the Accessibility Rule if that rule is amended while the Agreement is in effect. The Contractor agrees to complete and provide the City updated compliance report(s) upon request during the term of the Agreement, which may include updated versions of the VPAT that conform with any amendment to the Accessibility Rule, and to cooperate with the City’s compliance review process. Where the City issues stricter accessibility requirements in the solicitation or specifications, those requirements will also apply to the extent consistent with the Accessibility Rule.



Any claim of exception or undue burden under the Accessibility Rule must be documented by the Contractor with supporting facts and approved in writing by the City. The Contractor shall provide equivalent access consistent with the Accessibility Rule where an exception is applicable.

Failure to comply with this provision when required by the Accessibility Rule shall be considered a material breach and subject to termination of the Agreement upon written notice by the City. Alternatively, and without waiving any available remedy, the City may withhold payments due to the Contractor until compliance is achieved or the parties have agreed in writing on a plan to reach compliance or meet any applicable exception under the Accessibility Rule. Notwithstanding the foregoing and any other termination provision in the Agreement, the City shall provide Contractor not less than thirty (30) days to achieve compliance after written notice before withholding payment, and not less than forty-five (45) days to achieve compliance after written notice before termination for violating this provision.

Project Interrelationships

The City of Baltimore promotes equal business opportunity in the City's contracting process by encouraging full and equitable participation by minority and women's business enterprises. The Minority and Women's Business Opportunity Office's (MWBOO) authority to set MBE/WBE goals is governed by the Baltimore City Code [Article 5, § 28](#). No MBE/WBE participation goals have been established for this professional services solicitation.



This page intentionally left blank