**RFP 23-74658**

**ATTACHMENT I**

**MINIMUM REQUIREMENTS**

Please provide a yes/no (Y/N) in the blue shaded area below indicating your ability to meet requirements listed below and provided in supporting documentation as specified. **If an item is left blank, you will be implying that your company cannot meet the requirement(s), and your proposal may be eliminated from evaluation**. This document will be used to evaluate Respondents as described in RFP Section 3.2 (Evaluation Criteria), Step 1 (Adherence to Requirements). The numbered section headers are aligned with sections within the Attachment J Scope of Work.

|  |  |  |
| --- | --- | --- |
| **Item #** | **Requirement Description** | **Respondent Answer** |
| **General** | | |
| 1 | The State requires that the Respondent has experience supporting programs with over 300 websites, over 125 applications, and over 600,000,000 views per year. Provide documentation supporting the requirements in this section and denote the attachments in the “Respondent Answer” section. |  |
| **1.2.1.1.1 Organization Chart** | | |
| 2 | The State requires that the Respondent provide a proposed organization chart for the IN.gov Program, indicating which positions are considered Key Personnel, and describe the responsibilities of key positions and departments. The organization chart shall clearly delineate lines of authority and responsibility for all service areas. The Respondent shall also describe the benefits of such an organization and the time frame for implementation. |  |
| **1.2.1.1.2 Staffing Plan** | | |
| 3 | The State requires that the Respondent provide a staffing plan that identifies all of the personnel by position that the Respondent proposes and that are required to complete all requirements as outlined in this RFP. The staffing plan must include:   * A matrix matching each team member to the staffing requirements * A contingency plan that shows the ability to add more staff if needed to ensure meeting a requirement’s due date(s) * A statement and chart that clearly indicate the time commitment of the proposed team members during each phase of the Respondent’s proposed work plan * A statement indicated to what extent, if any, Key Personnel may work on other projects during the term of the Contract. The State may reject any Proposal that commits the proposed Key Personnel to other projects during the term of the contract, if the State believes that any such commitment may be detrimental to the Respondent’s performance. |  |
| **1.2.1.2 Subcontractors** | | |
| 4 | The State requires that the Respondent not use the experience or qualifications of a Subcontractor to meet any of the Minimum Requirements for Responsiveness outlined in RFP Attachment I1. These must be fulfilled exclusively through the qualifications and experience of the Respondent. |  |
| **1.2.1.4 Background Checks** | | |
| 5 | The State requires that the Contractor, at their own expense, undertake a criminal history record background check for all Contractor and Subcontractor personnel assigned to work on the contract. For all Contractor and Subcontractor personnel assigned to work on Day 1 of the Contract, the fingerprints required to complete the criminal history record background check shall be completed and reviewed by the Contractor by the 90th day of the Contract. |  |
| **1.2.2.1.1.1 Contractor Account Representative** | | |
| 6 | The State requires that the Contractor designate an individual who will be primarily dedicated to the State account (the “Contractor Account Representative”) who:Will be the primary contact for the State in dealing with the ContractorWill have overall responsibility for managing and coordinating the delivery of the services,Must meet regularly with the State Account Representatives and  * Must have the authority to make decisions and commit the Contractor’s firm with respect to actions to be taken by the Contractor in the ordinary course of day-to-day management of the Contractor’s account in accordance with this RFP. |  |
| **1.2.2.2.1 Issue Escalations** | | |
| 7 | The State requires that the Contractor provide an issue resolution process and escalation procedure that includes the following minimum requirements:Escalation matrix with escalation contact pointsEscalation paths for different escalation areas and levels (Critical, Urgent, Medium, Query)Impact assessment which explains the level of the issue (e.g. Statewide, multiple State entities, or only a single State entity)Initial response time frames and resolution time periodsA tracking system that assigns unique tracking IDs to each reported issue which will be maintained for the life of the contract.  * Monthly reporting of issue resolution status to the State contract administrator and to the State Entity(s) impacted |  |
| **1.3.1 Required Operating Environment & Infrastructure Technology** | | |
| 8 | If the Contractor elects to use hyper-scalers, the Contractor must utilize the State’s tenant. If the Contractor elects to host in the cloud, they must choose which of the State’s cloud tenants they will utilize between Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). The Contractor must manage their cloud environment within a carved-out space in the State tenant. The State shall bill the Contractor for their usage of the State’s tenant. |  |
| **1.3.1.2.2 Internet Bandwidth Support** | | |
| 9 | The State requires that the Data Center must support at minimum 100MB bandwidth with the ability to burst up to 20GB. All Data Center gear and ports must have the ability to burst up to 20GB. These data standards are calculated as the 95th percentile based on five-minute samples. |  |
| **1.3.1.4 Cloud Hosting** | | |
| 10 | The State requires that any cloud offering provided by the Contractor adhere to the security standards and requirements as outlined in Attachment M: IOT Cloud Provider Questionnaire. |  |
| 11 | The State requires that any cloud offering provided by the Contractor adhere to FedRAMP Moderate standards. |  |
| 12 | For Cloud Hosting Solutions, the State requires that the Contractor provide all of the technology infrastructure and all related managed services required to run and manage the application, including, but not limited to:  * Ensure infrastructure security aligns with IOT’s security policies * Provision of infrastructure capacity as needed * Provision of environments * Manage storage * Provide operating system, application and database backup and recovery services * Perform infrastructure capacity planning * Provide Level 2/3 support for infrastructure in accordance with the IOT’S incident management processes * Plan and execute required infrastructure changes in accordance with the IOT’S change and release management processes * Plan and execute infrastructure software updates into production * Maintain infrastructure configuration in accordance with IOT’S configuration management process * Ensure consistency and synchronization of disaster recovery environment with production environment * Participate in periodic (twice annual) disaster recovery testing * Manage disaster recovery infrastructure environment to meet Recovery Point Objectives and Recovery Time Objectives * Plan and execute OS and system utilities patches |  |
| **1.3.1.5 Operating Environment Changes** | | |
| 13 | The State requires that the Contractor schedule its implementation of System Environment Changes so as not to unreasonably interrupt State business operations. |  |
| 14 | The State requires that the Contractor make no System Environment Changes that would materially alter the functionality of the systems used to provide the services or materially degrade the performance beyond the established response times established by the SLA’s in Attachment L/Section: 1.6 without first obtaining State approval. In the case of an emergency, and in keeping with then-current State security policies, the Contractor may make temporary System Environment Changes at any time and without State approval, to the extent such System Changes are necessary, in the Contractor’s judgment, (i) to maintain the continuity of the services, (ii) to correct an event or occurrence that would substantially prevent, hinder or delay the operation of State critical business functions; and (iii) to prevent damage to the Contractor’s network. The Contractor must promptly notify the State of all such temporary System Environment Changes. At the conclusion of the emergency, the Contractor must restore any System Environment Changes to the pre-emergency state, and if the change is deemed necessary for normal operation of the system, a corresponding change request as outlined in Section 1.2.6 must be initiated for State review and approval. |  |
| 15 | The State requires that the Contractor review and perform a root-cause analysis of any deviation from scheduled System Environment Changes and failed System Environment Changes. |  |
| 16 | Prior to using any software or equipment to provide the services, the State requires that the Contractor utilize State defined testing efforts including all required testing with the exception of User Acceptance or Validation testing, which shall be performed by the State to verify that the item has been properly installed, is operating substantially in conformance to its specifications, and is performing its intended functions in a reliable manner in keeping with the defined Service Levels in effect at the time of the change. |  |
| 17 | The State requires that the Contractor follow a mutually agreed, formalized and published methodology in migrating systems, environments, configurations and Contractor supplied programs from development and testing environments into production environments. |  |
| **1.3.1.6 Code Based System and Environment Changes** | | |
| 18 | The State requires that for System Changes to any State system or environment within the Contractor’s scope of work that involve the change of code or data whether associated with IOT, the Contractor must:  * Establish, publish and maintain a formal release calendar in consideration of the scheduled or required changes to IOT; * Develop release packaging rules that include provisions for Contractor system and performance testing, State review and approval of Contractor results, and provisions for State acceptance or validation testing (depending on the nature of the change); * Operational procedures to backup or otherwise copy the IOP environment prior to implementing the change; * Change implementation roles and responsibilities prior to making the change; and * Rollback or reversibility considerations including success/failure criterion applicable to the change. |  |
| 19 | The State requires that the Contractor implement, utilize and maintain:   * Industry standard code management, version control tools based on the required change management suite and approved by IOT; and * Requirements traceability for all elements of a system change in alignment with Section 1.4.6-Change Management. |  |
| 20 | The State requires that the Contractor:   * Ensure that all changes adhere to State security, privacy and data handling policies; * Employ standard test beds that are utilized and extended for purposes of fully demonstrating completeness of adherence to business, functional and technical requirements at State required quality levels; * Utilize Contractor provided/managed automated methods and tools for accomplishment of routine testing functions, wherever possible; and * If applicable, include performance testing for high volume (transaction or data) transactions at the mutual agreement of the State and Contractor in consideration of the contents of a change. |  |
| **1.4.4.1 Project Development Lifecycle** | | |
| 21 | The State requires that for a period of two weeks after deployment, any issues/bugs found within the website/application shall be resolved, at no additional cost, by the Contractor. |  |
| **1.4.2 Documentation Requirements** | | |
| 22 | The State requires that the Contractor capture or create documentation for all project work, (whether work is performed under a SOW, TO, or CO), including establishing project specifications, milestones achievement, changes to specifications, acceptance of the final as-built project, approval for deployment, and agency acceptances as agreed to in the SOW, TO, or CO. The State also requires that the Contractor supply to IOT online access to all written materials, statements of work, task orders, meeting minutes, documents, and artifacts related to each phase of the project, including but not limited to a Risk Assessment Plan, Communication Plans, complexity assessments, and where applicable; user manuals; process and data flow diagrams and a Requirements Traceability Matrix. |  |
| **1.5 Reporting** | | |
| 23 | The State requires that the Contractor utilize Microsoft Project Online to complete their reporting duties, unless otherwise agreed to by the State. All reporting templates that the Contractor utilizes are required to be standard Microsoft Project Online reporting templates or templates that are otherwise agreed to by the State. |  |
| **1.5.1 Status Reports** | | |
| 24 | The State requires that the Contractor furnish the below status reports:  * Weekly Project Status Reports * Monthly Performance Reports (Including Third-Party Tools) * Monthly Late Log Reports * Project Staging Reports * Additional Management Reports * Financial Reports * IN.Gov Security and Privacy Reports * Credit Balance Reports (see Section 1.17.6.1) |  |
| **1.7 Training** | | |
| 25 | The State requires that the Contractor lead or assist the State with the following training activities:  * Provide staffing necessary to train Agency users in their application on an as-needed basis —both on demand requests for training and as part of an overall education plan in the case of newly supported tools. * Training options, including one-on-one, group training, and on-line tutorials should be made available in order to best meet the needs of Agency users. The Contractor shall provide the State with written training materials, including templates / guides of best practices and commonly-used code, that State users can independently reference. * Conduct web content management user training for State content managers and communicators, as well as Web Accessibility and SEO training for State Agency Users. (This enhanced offering should be available to Political Subdivision users through a Task Order). * Conduct an annual security training program for all web content managers * Develop and maintain user, provider, and operations manuals * Perform and/or enable baseline staff to attend or participate in applicable Web Portal-related trainings. * Trainings may be provided by the Contractor, the Contractor's parent company or an affiliate of the Contractor's parent company or otherwise deemed appropriate by the Contractor.  The State also requires that the Contractor develop and maintain a robust training plan that includes key objectives, training tools, roles and responsibilities, training environments, approach and methodology, training types, materials, effectiveness, and a description of how they will meet the requirements listed above. The Contractor must provide a sufficient number of staff to successfully accomplish all of the bulleted requirements, and this staff must have proven experience in the development and delivery of comprehensive training for a project of similar scope and scale. |  |
| **1.8 Help Desk and Customer Support** | | |
| 26 | The State requires that the Contractor provide staffing (e.g., customer service representatives) necessary to provide customer service help desk, billing support, and technical support for all applications and services built and/or maintained by the Contractor. The Contractor must also have the ability to ramp up support during peak usage times, such as during tax season, to ensure its ability to handle any potential increase in support call volume. |  |
| **1.9 Marketing** | | |
| 27 | The State requires that the Contractor proactively market and promote to agencies the benefits and use of IN.gov portal services as part of an overall agency Technology Needs Assessment/Support Plan that must be updated and shared with IOT at least once a year. |  |
| **1.11.4 Security, Risk Monitoring, and Assessments** | | |
| 28 | The State requires that, as a part of ongoing security support, the Contractor:  * Inform the State of both offensive and defensive security strategies in place in the Contractor’s environment * Complete and deliver a formal security risk self-assessment of the Contractor’s environment, with a strategy and action plan to address identified risks * Deliver updates to the assessment to the State security staff quarterly until all identified risks are resolved * Conduct comprehensive manual and automated reporting of the technical environment(s) that house State applications regularly, the results of which must be provided to the State at least monthly, and on demand by the State when necessary * Communicate to the State, in writing, any changes to the threat landscape that could reasonably and materially impact the State, including advice on action to be taken by the State if required * Participate in quarterly meetings with designated State security staff to provide security activity updates. |  |
| **1.11.6 Security Plan** | | |
| 29 | The State requires that the Contractor utilize a security testing approach that aligns with NIST 800-115, Technical Guide to Information Security Testing and Assessment. |  |
| **1.11.7 Audit Controls** | | |
| 30 | The State requires that the Contractor’s portal support provide the capability to maintain access roles that dictate the permissions for system and application access. The State also requires that the Contractor make audit reports and risk mitigation plans available for review by the State one month after completion. |  |
| **1.11.8 User Accounts** | | |
| 31 | The State requires that user accounts follow the password complexity requirements of IOT. Accounts with privileged access which are authenticated by the Contractor are required to have at least NIST 800-63 AAL-2 authentication. The State requires that password hashing adhere to NIST 800-63B Section 5.1.1.2. |  |
| **1.11.10 Protection of Personally Identifiable Information** | | |
| 32 | The State requires that the Contractor provide a system that shall encrypt all financial and confidential data transmissions. The State also requires that all data movement within or out of the State environment utilize an approved State provided process. |  |
| **1.11.11 Privacy** | | |
| 33 | The State requires that the Contractor maintain a Privacy Incident Response Plan, either as a standalone document or as part of its current Security Incident Response Plan, a copy of which must be shared with the State for its review. The Plan shall be reviewed and updated annually. |  |
| 34 | If the Contractor handles federal tax information (“FTI” – defined in IRS Publication 1075, §1.4 [November 2021]), the Contractor is required by the State to comply with applicable NIST and IRS Publication 1075 security controls and requirements to which the State subscribes. More specifically, if the Contractor handles FTI for the Department of Revenue, then the Contractor is required by the State to comply with all applicable aspects of the NIST 800-53 pertaining to safeguarding such data. |  |
| 35 | The State requires that the Contractor house all data in the continental United States. |  |
| **1.12.1 Website Staffing** | | |
| 36 | The State requires that the Contractor provide a Creative Services team that includes a dedicated Senior Creative Manager with experience using UI/UX design. |  |
| **1.12.3 Website Design Tasks** | | |
| 37 | The State requires that the Contractor maintain a response time of at least 200 milliseconds but no more than 1 second for all web pages and report response time. |  |
| **1.12.5 Content Changes** | | |
| 38 | The State requires that the Contractor utilize the State’s help desk solution software for managing content changes. Every request must be logged through the State’s help desk solution software. |  |
| **1.13.2 Operational Requirements** | | |
| 39 | The State requires that the Contractor manage all aspects and provide on-going support of the State’s web content management system, WebCMS. |  |
| 40 | The State requires that all websites and applications incorporate and link to the State’s Enterprise Web Analytics tool as part of the design. |  |
| **1.15.1 Application Software** | | |
| 41 | The State requires that the Contractor meet the following standards for applications developed by themselves for deployment by the State:  * Security credentials are built into each newly-developed application * Application access to databases is based on user credentials or service accounts * All applicable and relevant PCI DSS security requirements are met for applications performing payment processing |  |
| **1.15.3 Application Programming and Development** | | |
| 42 | The State requires that the Contractor:  * Conform to applicable industry practice in its application development. All applications are required to be developed based on secure coding guidelines such as the Open Web Application Security Project Guidelines ("OWASP") Top 10 and the CWE/SANS Top 25 Programming Errors published regularly by the SANS Institute. * Use application scanning software and a process to promote the release of secure code at the time such code is put into production. * Use commercially reasonable efforts to implement appropriate changes needed as a result of updates published to the guidelines. * Adhere to all applicable Standards (State, SOX and PCI DSS) for all Application Development. Should the State request access to any data covered by PCI DSS, then State compliance with PCI DSS requirements is a necessary precondition to Contractor compliance. * Use commercially reasonable efforts to ensure that the hardware, software and services provided to or purchased by the State from the Contractor are compatible with the principles and goals contained in the electronic and information technology accessibility standards adopted under Section 508 of the Federal Rehabilitation Act of 1973 (29 U.S.C. 794d). * Conform to Information Assurance Support Environment (IASE) STIGs Application Security & Development for all major application changes to existing application and new application development devours. * A comprehensive source code scan (using guidance from SANS, OWASP, and other nationally or internationally recognized sources) of all applications is completed on an annual basis. Designated State security staff members must review the proposed scan methodology before a source code scan. Upon request, the scan’s results must be delivered to and reviewed with the State * The Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines (WCAG) 2.0, Level AA (ISO/IEC 40500:2012), which reflect administrative rules on IT accessibility, are followed by the Contractor. |  |
| **1.15.6 Application Repository and Source Code** | | |
| 43 | The State requires that the Contractor build and maintain an applications and services library where the data is backed by a data store and is manageable online. This library is required to list all applications used in connection with IN.gov and be designed to grow over time. The applications inventory data is required to be housed via an online database with the backend database hosted at IOT, and it must be audited and updated no less than quarterly and readily accessible by the State. |  |
| **1.16.1 Third-party Applications - General** | | |
| 44 | The State requires that the Contractor maintain version control history and documentation for all IN.gov supported, third-party portal service applications. |  |
| 45 | The State requires that the Contractor provide, manage and maintain third-party portal managed applications that support the following IN.gov functionality:Calendar & Events RegistrationAccessibility and Quality AssuranceAccessibility Screen ReaderAutomated Web Accessibility ToolURL ShortenerContent Management SystemWebsite Search ToolWebsite AnalyticsCustomer Identity and Access Management (CIAM) PlatformMapping Development Tool for Web Development (Note: the State’s GIS tool will be the primary tool used for mapping)FAQ SolutionChat Bot and Live Chat SolutionUser TestingWeb-based Org Chart SolutionForm and Workflow Builder and Management SolutionMobile Application SolutionsSubscription Service for Website Stickers and IconsApplication Style GuideStandard Application HeaderTraining for all Third-Party Applications or First-Party Solutions |  |
| **1.16.2 Third Party Application Hosting** | | |
| 46 | The State requires that the Contractor follow the procedures identified below to achieve the goal of providing easier support for third-party applications hosted on the IN.gov Infrastructure:The Contractor shall test applications provided by third parties and proposed for deployment on IN.gov for the limited purpose of determining whether they appear to conform to IN.gov deployment standards.The Contractor shall provide infrastructure support and coordination for third parties that may deliver an application in order to leverage a Contractor-deployed enterprise service, such as payment processing on IN.gov. The Contractor shall provide consulting on how to interface with any of the Contractor’s enterprise services, but shall not customize or change those systems or services to interface with a third-party application.The Contractor shall provide communications and hosting support for any Contractor-built service that interfaces with, or utilizes, a third-party application. The Contractor shall cooperate with other vendors that may provide those third-party back-end systems to make the Contractor’s systems compliant with other third parties. If a Time & Materials project requires an interface to a third-party application, the Contractor shall price the support and communication utilizing the Future Work Rate Card. |  |
| **1.17.1 Account Database or System** | | |
| 47 | The Contractor shall provide the State with a system that can manage the data sales program, including user transactions with the State of Indiana and user accounts associated with those transactions and a dedicated Subscriber Center, that allows businesses, government entities, schools, or individuals to subscribe to Web Portal premium services. |  |
| 48 | The State requires that the Contractor’s quarterly report to the Data Sales Oversight Advisory Committee contain the following:  * Agency/entity-specific breakdowns of data sales * Results of quarterly account audits (e.g., a quarterly audit report) * New bulk data and subscription requests that will be voted on by the Committee * Other information as directed by the Committee |  |
| 49 | The State requires that the Contractor’s Account Database or System allow for the viewing of transaction level detail and reports by agency and/or service. |  |
| 50 | The State requires that the Account Database or System have mechanisms to log and bill transactions (including for auto-payment users), track recurring transactions, generate and distribute invoices, develop transaction memos (and tie them to user IDs), reconcile payments, and authenticate and authorize users for application use. |  |
| **1.17.1.2 Access Types** | | |
| 51 | The State requires that the Contractor’s Account Database or System ensure that there are separate access levels that can be assigned (in accordance with this section) and are aligned to the type of data that can be obtained by the user. |  |
| 52 | The State requires that potential users be properly vetted and must receive direct approval from the State to be granted these access levels. |  |
| **1.17.1.3 User Authorization Procedures** | | |
| 53 | The State requires that the Contractor ensure their Account Database or System restricts user access to data that requires special authorization until it has been granted by the State. |  |
| 54 | The State requires that the Contractor vet users seeking special authorizations to ensure they meet the data management and sales program requirements and present their evaluations and recommendations to the State. |  |
| **1.17.3 Data Management and Sales Integrity and Auditing** | | |
| 55 | The State requires that the Contractor alert the State to any data management and sales program or Account Database or System irregularities, risks, or issues as soon as they are discovered. |  |
| 56 | The State requires that the Contractor include the results of a quarterly account usage audit in their quarterly report to the Data Sales Oversight Advisory Committee. |  |
| 57 | The State requires that the Contractor’s Account Database or System keep track of all defaulted or suspended users. |  |
| **1.17.4 Data Management and Sales Growth and Outreach** | | |
| 58 | The State requires that the Contractor’s plans, strategies, and mechanisms be clearly defined in the Contractor’s Marketing and Outreach Plan. |  |
| **1.17.5 Current State Agency Specifics** | | |
| 59 | The State requires that the Contractor modify or develop new Subscriber Center services at no additional cost to the State upon request by a State agency and approval by IOT. |  |
| **1.17.6 Invoicing, Fee Handling, and Annual Subscription Fee** | | |
| 60 | The State requires that the Contractor’s database or system to aggregate all fees and processed transactions clearly define the user who completed the transaction, what transaction was completed, and the total amount due for the transaction. At the end of each month, the Contractor is required to generate and send invoices electronically. |  |
| 61 | The State requires that the Contractor be responsible for working with the State’s payment processing vendor to process account payments made by EFT or credit cards, disbursing such funds to the depository designated by the Treasurer of State, and providing reports on all disbursements. |  |
| **1.17.6.1 Transaction Fees** | | |
| 62 | The State requires that all transaction fees be collected and passed through directly to the State by the Contractor. |  |
| **1.18 Quality Assurance** | | |
| 63 | The State requires that the Contractor must have a dedicated Quality Assurance (QA) team, which will be responsible for developing and establishing quality assurance standards and measures for the information technology services within the Contractor’s organization for the IN.gov portal. The State also requires that the Contractor maintain a test environment for testing all IN.gov supported third-party portal-managed application updates and upgrades prior to release. |  |
| **1.20 End of Contract Turnover** | | |
| 64 | The State requires that the Contractor set procedures in place to ensure a seamless transition and uninterrupted service throughout the transition to a project successor at contract end. By the end date of the Contract, the Contractor is required to turn over all State property to the State. |  |

If Respondent is unable to respond **YES** to all Minimum Requirements but believe they have an alternative solution, please provide the Item Number and alternative solution with an explanation. Alternatives will be reviewed and considered by the State as to whether they satisfy the minimum requirements.

**Alternative Solution(s) – If Applicable**

|  |
| --- |
|  |