**RFP #23-74658**

**IOT Web Portal**

**Attachment J: Scope of Work**

* 1. **Introduction and Background**
     1. **IN.gov Background**

The State of Indiana has made a significant investment in developing and deploying the IN.gov Web Portal. The State’s Web Portal has been in existence for over twenty-five years. The current IN.gov Web Portal includes more than 250 State websites, 60+ Local websites and 150 online services.

Current State Web Portal operations management includes datacenter hosting, website production, and outward facing web-based application development. Respondents shall be required to provide executive oversight, business analysis, project management, design, development, quality assurance, security monitoring, and customer service in support of the IN.gov Web Portal. In particular, the State’s Program has the following dynamics that Respondents must be in a position to address and enhance:

* Increase the State’s capabilities by deploying high impact and cost-effective systems and systems management capabilities;
* Differentiate the State wherever possible by providing unique offerings to State employees and State constituencies while providing best-in-class operational performance and capabilities;
* Support the migration of services to a reliable, repeatable and world-class set of operating capabilities, standards and methods that are delivered in a cost-effective and predictable manner;
* Maintain a Program that is designed to drive overall consistency of operations through the leverage of common systems platforms, consistent business processes and deploying/leveraging best practices wherever possible; and
* Work with the State to operate modern capabilities, delivered under contemporary IT standards, software and testing capabilities, and structured software development/implementation methodologies to ensure overall quality, operational agility, and alignment while supporting future requirements of the State in a reliable and cost-effective manner.

The State is seeking to contract with a full-service Respondent(s) to provide the services necessary to continue IN.gov Web Portal operations as they stand today and expand such services to meet future needs.

The State desires an all-inclusive pricing structure for all hardware, software, and personnel services required to maintain all IN.gov Web Portal services, applications and environments known here to forward as Baseline Services. Unless expressly stated otherwise, Baseline Services shall include all requirements set forth in this Attachment-J Scope of Work. Legacy and custom applications are not included within the scope of Baseline Services for this RFP. At IOT’s sole discretion, the Successful Respondent may be engaged to develop, modify, enhance, rewrite, and replace legacy and custom applications.

The State has provided as part of this RFP a representative listing of Attachments and Exhibits that are pertinent to the current and historical operating environment. Respondents are advised to review this information carefully in consideration of responding to this RFP.

* 1. **Contractor Obligations and Staffing Requirements**
     1. **Account Management and Staffing**

The Contractor’s staff shall be sufficient to perform the Baseline Services outlined in the RFP. This staff shall be comprised of full-time equivalent (FTE) persons, all of whom must be legal residents or citizens of the United States.

The Contractor shall be responsible for complying with all recommendations, protocols, recordkeeping requirements and best practices called for by such persons. The employees of the Contractor and subcontractors engaged by the Contractor shall be available to IOT at all times to respond to both routine and emergency situations encountered by the Contractor, and shall be made available to consult with and meet with the State as reasonably requested.

Contractor and any Subcontractors must execute all projects in the US. No offshore resources shall be allowed to work on any IN.gov or State Entity User project. Third-party resources shall be approved at the discretion of IOT prior to engagement.

* + - 1. **Staffing**
         1. **Organization Chart**

Respondent must provide a proposed organization chart, 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. Respondent shall also describe the benefits of such an organization and the time frame for implementation.

The organization chart shall include a dedicated Account Management Team, led by the Contractor Account Representative as outlined in Section 1.2.2.1.1.1- Contractor Account Representative, that shall serve as the single point of contact for the State. The Account Management team shall consist, at a minimum, of Key Personnel and Baseline Service staff positions with subject matter expertise in the following areas:

* Executive Leadership
* Application Infrastructure
* Application Architecture Development
* Web Design
* Project Management
* Systems Administration
* Organization Readiness
* Security
* Quality Assurance / Accessibility
* Customer Service
* Help Desk Support and Issue Resolution
* Accounting
* Privacy
* Legal
* Human Resources
* Marketing
* Customer Experience Team
  + - * 1. **Staffing Plan**

Respondent must 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 show each individual’s responsibilities for the requirements and identify proposed key personnel. It is highly desired for key personnel to be located in close proximity to the Government Center Complex so that baseline employees are available to meet in person with IOT and state agencies on short notice.

In addition, the plan must have the following information:

* 1. A matrix matching each team member to the staffing requirements in this RFP;
  2. A contingency plan that shows the ability to add more staff if needed to ensure meeting the requirement’s due date(s);
  3. A statement and a chart that clearly indicate the time commitment of the proposed team members during each phase of the Respondent’s proposed work plan; and
  4. The Respondent also must include a statement indicating 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. **State Resource Usage Guide**

The Respondent must submit a Resource Usage Plan, using RFP Attachment N- Resource Usage Guide, that provides a high-level understanding of required resources for Contractor, IOT, and State Entity User by functional area (e.g., Development & Configuration, Training, Testing, etc.). Respondent shall provide the number of hours the Respondent expects to commit to the project and the number of hours estimated for IOT and State Entity User resources.

* + - 1. **Subcontractors**

The Respondent may not use the experience or qualifications of a subcontractor to meet any of the Minimum Requirements for Responsiveness outlined in RFP Attachment I- Minimum Requirements. These must be fulfilled exclusively through the qualifications and experience of the Respondent.

If the Respondent seeks to meet any of the other qualifications and experience through a subcontractor, the Respondent must identify the subcontractor by name in the appropriate part of the proposed organization chart.

Respondent shall provide a list of the subcontractors, as part of the proposed organization chart, who will provide goods or services under the Agreement. The Contractor shall assume responsibility for all subcontractors.

* + - 1. **Third-Party Vendors**

The Contractor must share all contracts they have with third-party vendors that support any aspect of the IN.gov Program along with any changes that could impact the Contractor’s agreement with the State.

* + - 1. **Background Checks**

As a condition of employment and for purposes of determining a person's qualifications for employment, the Contractor shall, at their own expense: undertake a criminal history record background check for all Contractor and subcontractor personnel assigned to work on the contract. Starting from day one of the contract and continuing until the contract is no longer in effect, all employees must have undergone a fingerprint based criminal history check within 60 days of being assigned to this account. The Contractor shall notify IOT in the event a background check results in a conviction finding. IOT shall determine if the Contractor employee shall be removed from the assignment.

The criminal background check shall encompass the following areas:

1. Convictions of any State or Federal crimes shall be considered if they are deemed to demonstrate a nexus to the work duties assigned to the Contractor staff Referenced under: IC 10-13-3-33.5; IC 4-13-2-14.7; IC 4-15-22-10; IC 4-15-22-30; IC 12-24-3-2; IC 22-5-1.7; IRS Pub. 1075; HEA1079-2017; Arrests & Convictions Policy
2. Exclusions by the US Office of Inspector General
3. The Contractor shall be required to retain the results of an individual's criminal history background check as long as that person is assigned to the Contract. If a currently assigned individual is promoted to a role having increased responsibility, the Contractor shall, at its own expense, perform a new background check. The results of the criminal history background check shall be made available to IOT upon request. If a conviction has been found in the subsequent background check to be related to the new role of increased responsibility, then the Contractor shall notify IOT. IOT shall determine if the Contractor employee shall be removed from the assignment.
4. If the Contractor has had a State Police fingerprint based criminal history check performed for the employee that meets the exact criteria specified above, the check may be accepted by IOT at the State's sole discretion. Any such reference checks must have been done within six months of the contract start date.

Contractor shall require that its employees are responsible for reporting to their supervisor any arrests or convictions within five (5) calendar days from the date of the arrest or conviction. Contractor shall ensure the enforcement and administration of this provision and shall notify the State, via State Account Representative within two (2) business days of being made aware of such arrest(s) and/or conviction(s).

* + - 1. **Confidentiality and Non-Disclosure Agreements**

The Contractor shall obtain from its employees, subcontractors, independent contractors executed non­disclosure agreements. The Contractor shall require its employees, subcontractors and independent contractors to comply with any privacy or confidentiality requirements specified in an agreed-upon Statement of Work, Task Order or Change Order prior to beginning work on the particular project.

* + - 1. **Evergreen Personnel Considerations**

In an effort to foster a mutually supportive and collaborative environment in which the services are provided in an effective manner that drives value to the State, the Contractor and IOT will jointly review the performance of certain Key Personnel and Baseline Services positions, including the Contractor Account Representative.

* + - * 1. **Staffing Replacements and Substitutions**

The Contractor must provide, on a cadence set by the State, a current organizational chart and staffing plan identifying all Baseline Services staff, contract resources and their start dates, and each person's responsibilities and make available to IOT upon request. The Contractor shall provide the State with a copy of the resume of each new Baseline Services employee at the time it makes an offer of employment, and shall personally introduce each new Baseline Services employees to IOT's representatives at the regularly scheduled meeting following the date the employee starts work for the Contractor.

The Contractor shall execute its responsibilities by following and applying the technical requirements, guidelines and standards in all cases in a professional and timely manner. If the State becomes reasonably dissatisfied with the work product of or the working relationship with those individuals assigned to work on the IN.gov Web Portal, the State may request in writing the replacement or reassignment of any or all such individuals and the Contractor must either replace or reassign such individual.

* + 1. **Program Management and Governance**

IOT has operational and contract governance responsibilities for the IN.gov Web Portal and supporting services. IOT desires to establish a program management and contract governance model to ensure IOT State Entity User objectives are continually met through a healthy relationship with the Contractor. The governance model is a set of defined interactions, expectations, decisions, roles, and processes that guide the governance of IN.gov Web Portal services. The governance model is designed to be informed of the overall service operations while facilitating the effective resolution of issues and enabling strategic decision-making. This governance model shall include:

* 1. General Oversight of the program, including Administration and invoicing for services performed
  2. Governance (advice, counsel, and feedback to IOT and the IN.gov Web Portal to enhance planning, proposal development, and decision-making)
  3. Oversight of adherence to contractual requirements
  4. Decisions related to data ownership, financial oversight and reporting of Contractor services, and general management and decisions that cross program areas and/or impact multiple State Entity Users.
  5. Implementation of a governance structure to drive process improvements and consistency across the State
  6. Conduct compliance related certifications and annual audits
  7. Provide program level communications and reporting
  8. Monitor and Manage Service Level Agreement (SLA)
  9. Production and maintenance of development, design, architecture, security, and privacy standards
  10. Reporting including a quarterly best practices report comparing IN.gov functionality with other states
      + 1. **Governance Structure**

Operational governance consists of day-to-day management of the IN.gov Web Portal services, program-level communications, issue resolution, contractual and funding oversight, and customer satisfaction. Success with the IN.gov Governance Model rests largely on the effective management of operational processes that are the responsibility of the Contractor to establish and operate in conjunction with IOT and the State Entity Users. This close relationship between the Contractor, IOT, and State Entity Users provides an efficient working and operational governance foundation to foster quality services, including resolving issues and making in-scope decisions at the lowest possible level. It is expected that nearly all issues are resolved through direct interaction between the Contractor and State Entity Users with IOT executive leadership participation only for escalated issues as appropriate.

* + - * 1. **Key Governance Staff Roles**

**Contractor Account Representative**

During the Contract, the Contractor must designate an individual who will be primarily dedicated to the State account (the “Contractor Account Representative”) who (i) will be the primary contact for the State in dealing with the Contractor, (ii) will have overall responsibility for managing and coordinating the delivery of the services, (iii) must meet regularly with the State Account Representatives and (iv) 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.

**State Account Representative**

During the Term of the Contract, the State shall designate a senior level individual (the “State Account Representative”) and suitable alternates to perform this role in the event of vacation or absence who (i) shall be the primary contact for the Contractor in dealing with the State under this RFP, (ii) shall have overall responsibility for managing and coordinating the receipt of the services, (iii) shall meet regularly with the Contractor Account Representative and (iv) shall have the authority to make decisions with respect to actions to be taken by the State in the ordinary course of day-to-day management of this RFP. This Role shall provide the overall leadership and coordination for strategic governance of IN.gov services including:

1. Define the strategic business direction of Services
2. Resolve business critical issues escalated from IOT State Entity Users
3. Monitor implications of results for business performance
4. Ensure strategic goals are achieved
5. Approve changes to governance decision-making framework for services
6. Approve the addition or deletion of services
7. Approve changes to the service delivery model
8. Monitor service delivery and performance
9. Resolve issues with broad enterprise financial implications
10. Approve critical security or technology-related decisions
11. Consult on analysis of Customer satisfaction survey results and action plans
12. Review and approve changes to Service Levels, services, and performance reporting to align with business requirements
    * + 1. **Performance Management and Issue Escalation**

The governance model strives to resolve issues at the operational level. However, not all issues will be resolved at this level. The governance model shall include a mutually agreed upon escalation process designed to route the issue promptly and efficiently to the appropriate party for resolution.

* + - * 1. **Issue Escalations**

The Contractor shall provide an issue resolution and escalation procedure that includes the following requirements:

* 1. Escalation matrix with escalation contact points
  2. Escalation paths for different escalation areas and levels (Critical, Urgent, Medium, Query)
  3. Impact assessment which explains the level of the issue (e.g. Statewide, multiple State entities, or only a single State entity)
  4. Initial response time frames and resolution time periods
  5. A tracking system that assigns unique tracking IDs to each reported issue which will be maintained for the life of the contract.
  6. Monthly reporting of issue resolution status to the State contract administrator and to the State Entity(s) impacted
     + 1. **Governance Meetings**

The Contractor shall conduct regularly scheduled operational meetings focused on service delivery, projects, project planning, services and planning, operational status, finance, or other topics. The meeting cadence shall be dictated by IOT and shall include at a minimum:

1. A monthly meeting among the State Account Representative, the Contractor Account Representative and any other appropriate operational personnel to discuss daily performance and planned or anticipated activities that may adversely affect performance or any contract changes.
2. A quarterly strategic executive meeting to ensure the visions of the Contractor and State are aligned.
3. An annual senior management meeting to review relevant performance and other issues.

Meetings shall include the following topics:

1. Open and honest bi-directional feedback as to overall Service performance
2. Contractor/State working relationships
3. Contractor personnel matters
4. Replacement or augmentation of Contractor Staff
5. Contractor support (or lack thereof) of State initiatives
6. Opportunities for refinement or enhancement of services or service quality and other matters as appropriate

For each such meeting, upon the State request, the Contractor must prepare and distribute an agenda, which shall incorporate the topics designated by the State. The Contractor must distribute such agenda in advance of each meeting so that the meeting participants may prepare for the meeting. In addition, the Contractor must record and promptly distribute minutes for every meeting for review and approval by the State.

The Contractor must notify IOT’s IN.gov Web Portal management team in advance of scheduled meetings with stakeholders or designated alternates (other than meetings pertaining to the provision of specific services on a day-to-day basis) and must invite IOT’s IN.gov Web Portal management team to attend such meetings or to designate a representative to do so.

* + - 1. **State Entity User Technology Needs Assessment and Support**

The Contractor shall meet with current and prospective State Entity Users supported by the IN.gov Web Portal as deemed necessary in its good faith and reasonable discretion, and shall discuss findings with IOT at the regularly scheduled update meetings including:

1. Review Contractor services and identify any issues or problems
2. Market and promote the benefits and use of IN.gov portal services
3. Assess State Entity User needs as they relate to their core business and related services provided through IN.gov
4. Discuss current and future projects to meet their business needs
5. Assess the existing services provided by the Contractor to see if there are any issues or needs for a technology refresh

The goal of these meetings is to determine how the Contractor, and ultimately IN.gov Web Portal, can better serve the State Entity Users and their needs.

* + 1. **Pricing Structure**

The State desires an all-inclusive pricing structure for all hardware, software, and personnel services required to maintain all IN.gov Web Portal services, applications and environments known here forward as Baseline Services. The Contractor’s services delivered under this structure are to be resilient, secure, and meet the Service Level Agreements outlined in Attachment L.

* + - 1. **Organization of Service Areas**

In general, there are four areas under which the Contractor services are delivered, which are outlined below for Respondents’ understanding:

1. **Baseline Services**: Services and operations designed to support the ongoing operations of the Contractor provided/managed computing environments and solutions inclusive of all minor and major upgrades, third party applications, and personnel. Respondents must incorporate the costs of any third-party supplies and services in the baseline fees. Legacy applications are not included within the scope of Baseline Services for this RFP. At IOT’s sole discretion, the Successful Respondent may be engaged to develop, modify, enhance, rewrite, and replace legacy and custom applications. In such instances, the processes outlined in Attachment J – Section 1.2.3.1, #3 Future Work and the Rate Card as proposed in Attachment D – Cost Proposal will be utilized.

Hosting of third-party applications (those applications developed by someone other than the Contractor or its subcontractors or Affiliates) on the IN.gov Infrastructure for all Third-Party Portal Managed Applications and IOT third-party hosting requirements shall be included as part of Baseline Services. All other State Entity Users shall be given the option of Contractor hosting or IOT hosting for their Third-Party State Entity Managed Applications at the discretion of IOT after consulting with individual State Entity Users. In the event a State Entity User elects Contractor hosting, the Contractor shall bill the State Entity User directly using a Task Order and the proposed pricing in RFP Attachment D-Cost Proposal. Exhibit 6- Current Third-Party Hosting Requirements includes a listing of Baseline inclusion or State Entity User paid hosting requirements.

As part of Baseline Services, the Contractor shall maintain all current State Entity User websites. Exhibit 2- Current Website List and Exhibit 4- Political Subdivision Website List include listings of all current State Entity Users and listings of potential State Entity Users. As part of Baseline Services, the Contractor shall add up to 200 new Political Subdivision websites annually. Historically, 30-50 new Political Subdivision websites are added annually. Contractor shall not limit the addition of non-current State Agency websites included in Baseline Services. Historically, 5-10 State Agency websites are added annually.

As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to all State Entity Users if required.

* Calendar & Events Registration
* Accessibility and Quality Assurance
* Accessibility Screen Reader
* Automated Web Accessibility Tool
* URL Shortener
* Content Management System
* Website Search Tool
* Website Analytics
* Mapping Development Tool for Web Development (Note: The State’s GIS tool will be the primary tool used for mapping)
* FAQ Solution
* Form and Workflow Builder and Management Solution
* Subscription Service for Website Stickers and Icons
* Application Style Guide
* Standard Application Header

As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to all State Agency users if required. Political Subdivisions shall have the ability to access these at their own expense.

* Chat Bot and Live Chat Solution
* User Testing
* Web-based Org Chart Solution
* Mobile Application Solutions
* Additional Accessibility and WCAG Compliance Services

Respondents shall provide a fixed annual fee that incorporates all requirements outlined in this RFP and attachments for the ongoing maintenance and support of IN.gov Web Portal services, applications and environments. Where applicable, Baseline Service work shall be documented using a Statement of Work (SOW).

* 1. Baseline Services shall also incorporate a mutually agreed upon level of the following IN.gov Web Portal support elements. Any unused quantities shall carry forward into the following fiscal year. All quantities shall be utilized prior to contract close. In the event quantities are unable to be utilized, IOT and the Contractor shall determine a mutually agreed upon refund for all remaining quantities. Respondents shall include in their RFP Attachment D- Cost Proposal fixed annual figures for the following:
     1. The addition of new Third-Party Portal Managed Applications
     2. The addition of domain names

1. **Continuous Improvement Hours**: Minor alterations and enhancements (inclusive of analysis, design, construction, testing and implementation tasks) to infrastructure and application elements within the scope of the Baseline Services. The State may also request hourly consultative expertise services pertaining to business, functional or technical expertise from the Contractor. The Respondent must include, in their proposed annual cost for Baseline Services, an annual pool of six thousand (6,000) hours. Any unused hours will carry forward into the following fiscal year.
2. **Future Work:** The design, development, testing and deployment of new applications, including legacy applications, capabilities, or significant application or capabilities enhancements are not included within Baseline Services. The State expects that most work conducted as part of this Contract will be performed as part of Baseline Services. State Entity Users may request additional work to be performed under this Contract via a Time and Materials Task Order to fulfill in-scope requirements not offered via Baseline Services. Respondents shall provide a rate card to be utilized for all future work. Future work shall be mutually agreed upon by IOT and the Contractor and shall be documented using a Time and Materials Task Order (TO). The Contractor may not propose rates in any Time and Materials Task Order that differ from this rate card as allowed under any contract arising from this RFP.
3. **Political Subdivision Inclusions (Refer to RFP #23-74658 Section 1.2 for definition):** Services are to be provided to Political Subdivisions within the following classifications:
   1. Baseline Services: The following services shall be provided to any current or future Political Subdivisions as part of the fixed annual Baseline Services fee:
      * + Website development and hosting on the State standard templates
          - 4 support requests per customer/month
          - Online CMS training
          - Online Third-Party Portal Managed Application training
          - 10 CMS user licenses
          - 100 migrated/built pages
          - 4 Web based forms per year
        + As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to Political Subdivision users:
          - Calendar & Events Registration
          - Accessibility and Quality Assurance
          - Accessibility Screen Reader
          - Automated Web Accessibility Tool
          - URL Shortener
          - Content Management System
          - Website Search Tool
          - Website Analytics
          - Mapping Development Tool for Web Development (Note: The State’s GIS tool will be the primary tool used for mapping)
          - FAQ Solution
          - Form and Workflow Builder and Management Solution
          - Subscription Service for Website Stickers and Icons
          - Application Style Guide
          - Standard Application Header
        + The Contractor must market and promote the benefits and use of IN.gov portal services
   2. Additional Political Subdivision Services: The following services shall be extended to Political Subdivisions at mutually agreed upon prices:
      * + Application Development
        + Marketing and Graphics
        + Online/ web form design and access
        + Mapping Services (Note: The State’s GIS tool will be the primary tool used for mapping)
        + Upgraded support, including additional support tickets, migrated pages, forms, and customized training
        + Additional Accessibility and WCAG Compliance Services
        + Custom Web Portal consultation
        + Third-Party Portal Managed Applications:
          - Chat Bot and Live Chat Solution
          - User Testing
          - Web-based Org Chart Solution
          - Mobile Application Solutions

* 1. **Infrastructure**
     1. **Required Operating Environment & Infrastructure Technology**

Infrastructure Technology refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. This environment is currently designed to host and maintain for State Agency and Political Subdivision websites:

* All IN.gov supported applications
* Non-IN.gov supported, PCI compliant applications that interface with the Payment Processing Solution (Payment Processing services are provided under separate QPA Contracts and are not included in the scope of this solicitation unless expressly noted)
* All IN.gov web content
* All IN.gov supported Portal Services Software (third-party software as described in Section 1.16-Third- Party Applications)

As part of Baseline Services, the Contractor must provide any hardware and software needed to provide a separate development, test, quality assurance and production environment for the IN.gov Web Portal.

In an effort to reduce overall cost, improve capabilities, increase performance and reduce infrastructure oversight, the State is willing to consider Respondent offerings for both on-premise and cloud hosted environments. Respondents shall submit solutions for either or both as part of their response, in alignment with the following requirements and in alignment with FedRAMP Moderate standards. 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. Invoicing details related to billing for tenant usage shall be finalized with the awarded vendor prior to Contract finalization. However, in line with the State’s efforts to seek technological innovation in the IN.gov program, the Respondent may also propose an alternative cloud hosting solution along with their State tenant-hosted proposal. The Respondent must explain as part of this proposal why their alternative proposal would be more advantageous to the State. This opportunity does not guarantee that a Respondent’s alternative cloud hosting proposal will be accepted, and as such, pricing and proposal elements cannot be contingent upon acceptance.

* + - 1. **Infrastructure Technology Enterprise Architecture Requirements**

The Contractor shall comply with all IOT standards, policies and guidelines, which are online at https://www.in.gov/information-security-framework/. The Contractor specifically agrees that all hardware, software and services provided to or purchased by the State shall be 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) and Ind. Code§ 4-13.1-3. Any deviation from these architecture requirements must be approved in writing by IOT in advance.

* + - 1. **Internet Connectivity and Bandwidth**
         1. **Internet Connectivity**

The internet connectivity between the Data Center and the State and the Data Center and the user shall be provided and monitored by Contractor with respect to its sufficiency to handle IN.gov Web Portal traffic without significant degradation in IN.gov Web Portal performance. The Contractor shall be responsible for addressing and correcting any such deficiencies, including providing increased bandwidth, if necessary. Contractor shall not be responsible for issues associated with user's phone, computer, or communication device, power made available by the public utility or internet connections not maintained by Contractor.

* + - * 1. **Internet Bandwidth Support**

Communications between the Primary Host Data Center and any Back-up Host Data Centers to the State Data Center shall utilize Virtual Private Network (VPN). Standard traffic runs between 100 and 200MB with traffic bursts during peak times of up to 20GB. Host Data Center connections to the public must support at minimum 100 MB bandwidth with the ability to burst up to 20GB. All Host 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. **On-Premise Hosting**
         1. **Data Center Standards**

The Contractor shall be responsible for all fees and costs associated with the hosting of the IN.gov Web Portal at a primary facility with a secondary site with “warm” backup capabilities for non-critical systems and “hot” backup capabilities for critical systems at a location in the United States that is geographically remote from the primary site in or an Azure or Amazon Infrastructure as a service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) environment also at a location in the United States, or a hybrid solution. The Contractor and its proposed Data Center vendor (if applicable) are responsible for all hardware, network infrastructure, security infrastructure, server infrastructure, disaster recovery infrastructure and related tools and utilities necessary to support a web portal of this size and complexity.

The following represents key facets of the typical infrastructure required:

* Web Servers: 16 virtual servers (Production), 4 virtual servers (Test). This is subject to load, with the ability to ramp up if needed.
  + Applications servers are not included in this number, which is approximately 300 and growing.
* Load Balancers: 4 physical with additional virtual capability (2 physical appliances in each data center)
* Server Management Software and Tools Licensing:
* SQL Server Databases: 1 Development, 2 Quality Assurance (QA), 4 Production in a multi data center cluster.
* Additional Database: 1 Production Cluster hosted by the Contractor. IOT shall host the Production and Test Instance for IN.gov.
* Intrusion Prevention System
* Multi-Node Web Application Firewall
* File Upload Scanning Appliance
* Security Event and Incident Management (SEIM) Logging Tool
* Logging Software
* Virtual Hosts: 10 Hosts spread across two data centers
* EMC Storage: Multiple Storage Arrays split between two data centers
* Firewalls and Switches
* Internet Bandwidth supports 2Gbps and above in multiple data centers
* DDOS appliances in both data centers
* VPN connecting the primary vendor datacenter with the IOT datacenter

Note that, based on experience maintaining datacenters for similarly scaled portals, Respondents are encouraged to propose datacenter configurations that meet the State’s needs. IOT must approve of the brand and level of support for each.

* + - * 1. **Minimum Data Center Facility Standards (Primary and Secondary)**

IN.gov shall be hosted on a primary site with one back up site with "warm" back-up capabilities for non-critical systems and “hot” back-up capabilities for critical systems including websites and the content management system. These sites shall be located in no less than two (2) facilities. The Contractor shall provide the State with evidence that the Data Center either owns or has a lease on each of the facilities where hosting occurs. Key IOT or State employees shall be allowed to reasonably inspect each facility, no more frequently than once a year, and subject to the policies and procedures of the site. Arrangements at the Data Center shall be facilitated by the Contractor. Each of the facilities where IN.gov is hosted must meet the following minimum standards:

1. *Hardened Tier-3 facility* protected by multiple physical security measures, including (a) 24/7/365 on-premise security officers; (b) a facility command station; (c) continuous closed circuit video surveillance (interior and exterior); (d) security breach alarms; (f) electronic card key access; (g) with biometric device and individual personal access code; (h) secured cage and cabinet environment; and (i) measured against HITRUST CSF Control Specifications.

2. *Technical Support*, including (a) on-site building engineers monitoring all infrastructure systems (HVAC, power, fire suppression) 24x7x365; (b) redundant monitoring performed at separate network operations center; (c) immediate customer response through Remote Hands Technical Support and dedicated hotline notification; and (d) area for pre-installation and emergency maintenance activity.

3. *Fire Detection and Suppression*, including (a) Very Early Smoke Detection Apparatus (VESDA); (b) active laser air sampling system; (c) conventional smoke and heat sensors: cross-zone throughout the center on the ceiling, below the raised floor area, top of Computer Room Air Conditioning (CRAC) units, Uninterruptible Power Supply (UPS) room, etc.; (d) pre-action dry-pipe fire suppression system, or other equivalent industry standard.

4. *Air Flow and Cooling* must meet ASHRAE's "Thermal Guidelines for Data Processing Environments", or other equivalent industry standard.

5. *Power:* Minimum of N+1 Redundancy, including (a) four (4) separate UPS systems (2N redundancy); (b) replicated configuration for dual power feeds throughout facility; (c) fifteen (15) minutes of battery backup available at full load; (d) continuous monitoring of each battery bank; (e) mission critical generators with a minimum of International Organization for Standardization (ISO) rating of Emergency Standby (ESP) located either indoors or in effective outdoor enclosures, incorporating dual starter batteries, block heaters and at least 12 hours of outside fuel capacity.

6. *Continuous Upgrade Plan*, to include new technologies, improved or best practices that may develop during the term of the Contract, subject to the IN.gov Web Portal budget and other IN.gov Web Portal resources. The State shall be the beneficiary of all such upgrades as part of the Baseline Services.

* + - * 1. **Minimum Data Center Non-Facility Standards (Primary and Secondary)**

The primary and secondary data center shall each meet the following standards at a minimum:

1. The Data Center shall have the proven capability to achieve the 99.9% uptimes required by the State.

2. *Monitoring and Back-up.* The Contractor shall provide monitoring 24x7x365 using monitoring tools required and approved by the State. The Data Center shall provide near real time back up of the IN.gov static website content and all critical applications at its secondary site with no significant degradation of performance. Monitoring tools should include:

* SEIM: a SEIM tool that correlates logs from all security appliances as well as from web applications and web servers. Custom and standard logs shall be sent to the tool in real time. Logs should be continually reviewed by the Contractor. Alarms and reports shall be generated based on this data. Alarms are to be defined via contract as determined by the State. The Contractor’s SEIM tool must integrate with IOT’s SEIM tool.
* File Integrity Monitoring (FIM): a FIM tool to monitor file changes as well as network traffic to and from the server. Additionally, the tool shall track user access to the servers and report this information back to the portal’s SEIM tool.

3. *Distributed Denial of Service ("DDoS") Appliances.* The Contractor shall use commercially reasonable measures to manage and appropriately mitigate risks relating to DDoS attacks including but not limited to the following:

* Providing, managing and maintaining DDoS appliances in both data centers
* These services shall receive automated updates based on global threat subscriptions to support systematically blocking of IPs based on configured threat levels. The service shall provide country block lists as well as user supported block lists while supporting configuration details that can be fine-tuned for each service/domain.
* All logging shall be sent to the portal’s and IOT’s SEIM tool while daily, weekly, and monthly reports can be sent to executive staff.
* The Contractor shall provide the State with a report within 4 hours of identifying the issue detailing any significant DDoS activity, including how the DDoS activity was mitigated.

4. *Web Application Firewall (WAF)*

The Contractor shall utilize enterprise WAFs to block and log suspicious activity based on specific URLs and domains. The WAF configuration shall allow the portal to tune specific policies for each application or define an overall set of security rules for a domain. As an example, the WAF supports IP reputation, rate limiting, bot mitigation, and cookie and data field validation while receiving regularly scheduled security updates. The WAF protects traffic in both data centers while security logs are sent to the portal’s SEIM tool.

*5. Intrusions and Data Breaches- Intrusion Protection System (IPS)*. The Contractor shall have intrusion detection systems and intrusion prevention systems including but not limited to the following:

* IPS support in both data centers via data center grade firewalls
* The firewalls shall monitor and block traffic based on IOT approved IPS defined policies. These rules shall be routinely checked and validated as part of the Web Portal’s security program. Firewall and IPS policy blocks shall be logged and sent to the Web Portal’s and IOT’s SEIM tool.
* Any material reduction in the capabilities of these prevention systems shall only be made when the State has indicated that such change is acceptable to the State.
* Within 12 hours, the Contractor shall provide as much detail as is available at the time about the nature of any intrusion, and shall advise the State of all actions taken to mitigate.

6. *Incidents and Outage Response and Reporting*.

(a) In the event of a Service Outage to any critical system, the Contractor shall be responsible for contacting the State of Indiana within 1 hour of knowledge of an outage. The State shall be responsible for providing accurate contact information, including email addresses and phone numbers of appropriate designated employees. The Contractor shall be responsible for delivering an initial Incident Report to the State within 24 hours of knowledge of the incident; a detailed Incident Report must be submitted to the State within three business days after the Service Outage is initially resolved.

(b) All Incident Reports shall include the following details of the incident: Incident title with brief explanation, incident type (i.e., network), Severity, Internal or External impact, SLA-relevant, detailed explanation of incident and actions taken to resolve, State Entity User notification required, date, time, duration, trouble ticket number(s), final resolution, and an action plan to prevent reoccurrence.

(c) The Contractor shall maintain a current Escalation List, including all contact information, with the State.

(d) Monitoring and reporting of outages with respect to network services shall be conducted by an independent third-party service provider, reasonably acceptable to the State, using an industry-standard tool. The Contractor shall be responsible for the costs of the third-party provider's services, and the reports shall be made available to the State. Such reports shall be exempt from disclosure under Indiana's Access to Public Records Act, Ind. Code§ 5-14-3-4(a) and (b)(l0), (11) and (19).

* + - 1. **Cloud Hosting**

The Contractor may offer a Cloud Hosting future system to the State delivered as utilizing either an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a service (SaaS) configuration. The offering must be hosted within a State tenant. Any cloud offering must adhere to the security standards and requirements as outlined in RFP Attachment M: IOT Cloud Provider Questionnaire. Any cloud offering must also adhere to and align with FedRAMP Moderate standards. If the Contractor elects to host in the cloud, they shall 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 shall 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. Invoicing details related to billing for tenant usage shall be finalized with the awarded vendor prior to Contract finalization.

The Contractor must provide all of the technology infrastructure required (compute, network, storage, load balances, firewalls, etc.) and all related managed services required to run and manage the application. This includes, but is not limited to:

1. Ensure infrastructure security aligns with IOT’s security policies
2. Provision of infrastructure capacity as needed
3. Provision of environments
4. Manage storage
5. Provide operating system, application and database backup and recovery services
6. Perform infrastructure capacity planning
7. Provide Level 2/3 support for infrastructure in accordance with IOT’S incident management processes
8. Plan and execute required infrastructure changes in accordance with IOT’S change and release management processes
9. Plan and execute infrastructure software updates into production
10. Maintain infrastructure configuration in accordance with IOT’S configuration management process
11. Ensure consistency and synchronization of disaster recovery environment with production environment
12. Participate in periodic (twice annual) disaster recovery testing
13. Manage disaster recovery infrastructure environment to meet Recovery Point Objectives and Recovery Time Objectives
14. Plan and execute OS and system utilities patches
    * + 1. **Operating Environment Changes**

In order to mitigate potential risks and minimize the impact of changes to State operations, the Contractor must comply with the following control procedures for any changes to the Contractor provided/managed environments or supporting production infrastructure:

1. Contractor must schedule its implementation of Operating Environment Changes so as not to unreasonably interrupt State business operations.
2. Contractor must make no Operating 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 SLAs in RFP Attachment L- SLAs 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 Operating Environment Changes at any time and without State approval, to the extent such Operating 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 Operating Environment Changes. At the conclusion of the emergency, the Contractor must restore any Operating 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 1.4.6 - Change Management must be initiated for State review and approval.
3. The Contractor must review and perform a root-cause analysis of any deviation from scheduled Operating Environment Changes and failed Operating Environment Changes.
4. Prior to using any software or equipment to provide the services, Contractor must 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.
5. Contractor must 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. **Code Based System and Environment Changes**

For those System Changes (updates, upgrades, patches or otherwise) 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:

1. Establish, publish and maintain a formal release calendar in consideration of the scheduled or required changes to IOT;
2. Develop release packaging rules that includes provisions for Contractor system and performance testing, State review and approval of Contractor results, provisions for State acceptance or validation testing (depending on the nature of the change);
3. Operational procedures to backup or otherwise copy the IOT environment prior to implementing the change;
4. Change implementation roles and responsibilities prior to making the change;
5. Rollback or reversibility considerations including success/failure criterion applicable to the change; and
6. Collaborate with IOT to develop a cohesive SDLC process between the Contractor and the State.

The Contractor must implement, utilize and maintain:

1. Industry standard code management and version control tools based on the required change management suite and approved by IOT; and
2. Requirements traceability for all elements of a system change in alignment with Section 1.4.6 - Change Management.

The Contractor must:

1. Ensure that all changes adhere to State security, privacy and data handling policies;
2. 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;
3. Utilize Contractor provided/managed automated methods and tools for accomplishment of routine testing functions, wherever possible; and
4. 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. **Project Management, Change Management, and Release Control**

IOT uses a project management process, known as Project Success Center (PSC) Framework consisting of four phases: Initiating, Planning, Executing & Controlling, and Closing. Details on the PSC framework and requirements can be found at the following site: https://www.in.gov/iot/psc/. Contractor shall be responsible for adhering to the latest version of PSC standards.

While all projects will move through the aforementioned four phases to reach completion, the number and type of activities that a project team completes during each phase is determined by the project's classification. IOT has defined four specific complexity levels, each with its own project management requirements. Based on the project’s classification, the level of project management is scaled to the size and complexity of the project. This way, smaller, less complex projects require minimal or no formal project management while large, complex projects receive a more formalized project management structure and rigor.

The processes, procedures, and service levels in this Section apply to all project management undertaken by the Contractor. Where applicable, work included within the scope of baseline services shall be completed under a Statement of Work document. Work that is inclusive of requirements outside of the scope of baseline services shall be mutually agreed upon by IOT, the relevant State, and the Contractor as to whether the project shall be completed under a Time & Materials Task Order.

IOT utilizes a website, known as Webmasters.IN.gov, for the creation of project and task requests which subsequently flow into the IOT ticketing system. The Contractor shall be required, as part of their project management strategy, to access and maintain elements contained within the Webmasters.IN.gov platform. Contractor shall be required to manage all projects relating to content, applications, third-party applications, and vanity URL’s.

* + 1. **Complexity Levels**

The following table outlines the IOT established differentiating factors that shall be utilized to determine a projects complexity level. Complexity levels are categorized as: Basic, Low, Medium and High. Supporting details for each complexity level can be found at https://www.in.gov/iot/psc/.

|  |  |
| --- | --- |
| **Complexity Level** | **Project Description** |
| Basic | These types of projects are usually driven by an immediate business need to continue operations of an existing service or feature without further enhancements.  *Typical project duration: 1 day to 6 weeks*  *Time to develop charter:* *N/A*  *Size of charter:*  N/A  *Sample projects: Minor bug fixes, graphic updates,* content updates, |
| Low | These types of projects are usually driven by an immediate business need within a short timeframe and scope may involve multiple systems or State Entity Users but with a clear authority and a simple governance structure.  *Typical project duration:* 3 to 6 months with 2-5 resources  *Time to develop charter:* 8 to 20 hours  *Size of charter:*  1 to 3 pages  *Sample projects:*  New site setup, new functionality added to existing system |
| Medium | These types of projects usually involve more than one group or State Entity User and will include changes to both systems and business processes requiring a more complex governance structure, communication plan and risk management.  *Typical project duration:* 4 to 9 months with 3-10 resources  *Time to develop charter:* 16 to 24 hours  *Size of charter:*  5 to 10 pages  *Sample projects:*  Rollout of technology across multiple State Entity Users or locations, IOT support in complex enhancement or new State Entity User system (< 3-4 servers/databases) |
| High | These are complex projects that typically change fundamentals about the way the business area works and includes a large amount of new development/systems. They likely span organizational entities and involve multiple stakeholders, and require a complex governance structure.  *Typical project duration:* > 6 months with > 5 resources  *Time to develop charter:* 20 to 40 hours  *Size of charter:*  > 10 pages  *Sample projects:*  Implementation of new technology across all State Entity Users, IOT support of a large State Entity project (>$1M) |

* + 1. **Documentation Requirements**

The Contractor must capture or create documentation for all project work, (whether work is performed under a SOW, TO, or Change Order CO), including establishing project specifications, milestones achievement, changes to specifications, acceptance of the final as-built project, approval for deployment, and State Entity User acceptances as agreed to in the SOW, TO, or CO. The documentation will be created in coordination with and shared with the State Entity User (s) involved in the project and IOT.

The Contractor must supply to IOT online access to all written materials, SOWs, TOs, COs, 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. This documentation should be searchable by State Entity User and document title, and shall be deemed exempt from disclosure under Ind. Code § 5-l 4-3-4(a) and (b) (10), (11) and (19).

Documentation shall follow all guidelines as outlined at https://www.in.gov/iot/psc/. Documentation shall include but not be limited to the following documentation types:

* + - 1. **Project Charter**

A Project Charter lays the foundation of the project. IOT and State Entity User signoff on the charter allows the Contractor to begin billable work on the project.

* + - 1. **Statement of Work (SOW)**

Statements of Work shall be used for project requests initiated as part of Baseline Services. A Statement of Work (SOW) must be prepared by the Contractor’s project manager and approved by IOT before any non-emergency work requiring six or more weeks of work can be started. All other Baseline Services work of less than six weeks are initiated through a helpdesk ticket submitted in the State’s ticketing tool or included as part of the Weekly Status Report and presented at the regularly scheduled governance meeting with IOT.

All work performed under a Statement of Work must meet the performance criteria defined in RFP Attachment L - Service Level Agreements.

* + - 1. **Task Order (TO)**

A Task Order shall be used to document project requests that fall under Future Work Services as described in Section 1.2.3 - Pricing Structure of this RFP. Task Orders shall be mutually agreed upon by IOT and the Contractor prior to the commencement of work.

A TO must be prepared by the Contractor’s project manager for all Future Work Services and follow the appropriate approval processes as dictated by the sponsoring State Entity User and IOT and based on the source of project funding—State Entity User or the IOT. All TOs must:

* Follow the approach described in the project documentation based on the rigor defined by the project’s classification
* Be tracked in a like manner as part of a project portfolio management system
* Include a Risk Assessment to identify potential risks, their impact, and the likelihood of occurrence in order to determine the level of project management and oversight required for the project
* Include a Requirements Traceability Matrix
* Contain a not-to-exceed amount for the project, with hourly rates as set forth in the Contract

All projects completed under a TO must meet the performance criteria defined in RFP Attachment L- Service Level Agreements.

* + - 1. **Change Order (CO)**

A Change Order ("CO") request, must be used to document and authorize any changes to an SOW or TO and follow the change management procedures set forth in this section.

* + 1. **Standard Operating Procedure**

IOT and the Contractor shall agree on a standard operating procedure (SOP) for engaging the State Entity User. IOT shall approve the SOP and any changes to it in writing before implementation. All SOPs should include the following steps:

* 1. Use a Project Portfolio Management system (currently MS Project Online) to capture, manage, and measure the aspects of all projects collectively and individually.
  2. Complete a Project Request Form for each new application development project.
  3. Create documentation necessary to establish the required elements or specifications of project performance, including specifications, milestones achievement, changes to specifications, acceptance of the final as-built project, approval for deployment, and State Entity User acceptances as agreed to in the SOW, TO, or a CO. The documentation must be created in coordination with and shared with the State Entity User(s) involved in the project, with all final documentation and any related project changes delivered to the State.
  4. Provide a project schedule with dynamically-linked tasks that represents the work required to meet the requirements and deliverables of the project documented in the Project Charter.
  5. Provide a communications management plan addressing the needs of all relevant State Entity Users
  6. Ensure project requirements are traceable through the entire project lifecycle.
  7. Create and maintain a Risk Management plan for all projects over 1000 hours.
  8. Create and maintain a RACI diagram.
  9. Deliver all project documentation to IOT for review prior to delivery to any State Entity User .
  10. Prepare a list of all stakeholders, with definitions of the role and associated responsibilities of each.
  11. When a Project Charter is initially leveraged, estimate the amount of time it takes to complete a project schedule task as effort, in hours. The actual time shall be reported back to IOT and the relevant State Entity User via a project Task Order. The project Task Order will show what actually occurred during the project lifecycle.
  12. Add IOT as an optional attendee to every meeting it schedules with the State Entity User or stakeholder.
  13. Keep written meeting minutes documenting every meeting with an State Entity User or other stakeholder (whether or not related to project). The minutes shall document all commitments, decisions, or changes agreed to during the meeting. The Contractor shall create such minutes even if IOT personnel are in attendance.
      1. **Project Initiation**

All projects must be approved by IOT before the Contractor starts work. The overall planning and scheduling of application development work shall be under the direction of IOT with priority given to "one stop" customer-focused government services, cost reduction projects, State Agency­ funded projects and those governed by legislative changes. IOT has the authority to determine whether a project is a Baseline Service or will be done as a Time & Materials project with the mutual written agreement of the Contractor. Urgent Requests must be addressed as part of the regularly scheduled meeting with IOT in order to establish funding guidelines and obtain approval.

* + - 1. **Project Development Lifecycle**

IOT has developed the following Project Development Lifecycle:

1. Initiation
   1. Project Initiation: IOT shall approve the project request once received. Projects are requested via the Project Request Form found on the IOT project management system, WebMasters.IN.gov through the following link https://www.in.gov/iot/psc/start-a-project/. Once approved the Contractor shall review the project request form and determine whether to proceed as a project or convert it to a ticket within the WebMasters.IN.gov system. If it is determined to be a project, the Contractor shall assign a Project Manager (PM).
   2. Project Scoping: The PM shall gather necessary resources to begin scoping the effort inclusive of a kickoff meeting to gather high-level requirements, key milestones, budget, and a written business case.
   3. Project Charter: The Contractor shall use everything from the kickoff meeting, and any subsequent requirements gathering efforts, to estimate effort, cost range, and draft a charter. The Contractor and IOT shall mutually determine whether the project shall be included in Baseline Services or will be done as a Time & Materials project. The requesting entity shall either approve the charter, postpone, or cancel the project.
2. Discovery
   1. Project Discovery: If the charter is approved, the project team shall gather more detailed requirements from the requesting entity and associated stakeholders. A project backlog is created via User Stories and refined via feedback from the requestor.
   2. Project TO/SOW: Once the User Stories are approved by the requesting entity, a Task Order (TO) shall be created. The TO shall detail the scope of the project and include cost and project timeline information. A SOW shall be used if the project will be covered by Baseline Services, while a TO shall be used if the project will be done as a Time & Materials project and the Contractor will bill the requesting entity for time and materials. A TO or SOW can be modified utilizing the change management process outlined in Section 1.4.6- Change Management in the event that significant changes to scope are required.
3. Development
   1. Project Development: Upon requesting entity approval of the initial User Stories, the development of the requestor’s project request shall begin. This shall include additional User Story refinements as the product is being developed.
   2. Quality Assurance (QA) Testing: An internal quality check of the application shall be conducted inclusive of all requirements in Section 1.18- Quality Assurance to ensure all aspects of the project request are functional according to the documentation and the final User Stories.
4. User Acceptance Testing
   1. User Acceptance Testing (UAT): UAT testing begins on the application when it has passed the internal QA testing plan. UAT shall be conducted by the requesting entity team using their internal testing plan. The Contractor shall provide a UAT feedback document to track and resolve all UAT findings.
   2. Load Testing (optional): The Contractor can test the application to be sure it can handle a peak load of concurrent users. Load testing shall be done per State Entity User request. The State Entity User shall include in its request peak times the website/application will be accessed along with the expected traffic. This shall ensure the application is operating efficiently at all times.
5. Application Deployment
   1. Approval to Deploy: Once all the above steps are complete, the requesting State Entity User must provide final approval to launch the application.
   2. Deployment: The Contractor shall be responsible for scheduling and conducting the application deployment.
6. Warranty/Stabilization Period: For a period of no less than two weeks after deployment, any issues/bugs found within the website/application shall be resolved, at no additional cost, by the Contractor. This shall be a heightened level of support directly after go-live.
7. Support: Contractor must have a bug/issue tracking tool set that includes a robust dashboard for tracking defects, bugs and issues and communicating status. If any issues arise with the expected functionality of the website/application after the warranty period, the Contractor will continue to support the application at no cost. Support does not include enhancements or changes to the functionality of the website/application beyond the original commitment. Changes require a Change Order to be Submitted, while Enhancements shall require a new project request.
   * 1. **Project Close Out**
        1. **Close Out Survey**

Customer satisfaction is a critical component of the Contractor's performance. The State requires that a Customer Close-out Survey be completed as part of the Customer Satisfaction Service Levels. Acceptable Performance Levels shall be determined by an average of 90% of surveys to be no less than a "4 out of 5". The Contractor will create a report of recommendations to increase customer satisfaction based on the survey results and present this report to IOT at a cadence to be determined.

* + 1. **Change Management**

IOT uses a common change order process that includes a CO form, provides for State Entity User notification, and includes standard steps such as create, submit, review, approve or deny. The Contractor shall use documentation templates approved by IOT, and the Contractor shall follow approved processes similar to IOT project management.

* + - * 1. **Change Management Process**

IOT and the Contractor shall mutually agree on a Change Management Process in alignment with the Project Management requirements, tools and processes. The process should include, at a minimum, the following steps and/or key deliverables:

1. Notification
2. Documentation
3. Review, including cost estimation, risk assessment, and project impact evaluation
4. Approval
5. Implementation Schedule
6. User Testing/Acceptance
7. Deployment
8. Standardized methods and procedures to provide efficient and prompt handling of all changes
9. Schedule development, including approval, execution and implementation of changes
   * + 1. **Release and Deployment Control**

The purpose of Release Management is to build, test and deliver specified services that will accomplish the stakeholders’ requirements and deliver the intended objectives. The Contractor shall, at a minimum:

1. Work with IOT to develop and establish a Release and distribution process so that each change to services is controlled, tested, traceable, authorized, and implemented in a structured manner.
2. Conform Contractor operations to the mutually agreed upon Release policies, processes and procedures
3. Execute releases according to the approved Release Management methodology
   * + - 1. **Release and Deployment Control Process**

The Respondent shall propose a Release and Deployment Control process that includes, at minimum, the following:

1. Assign a Single Point of Contact (SPOC) for each Release being requested
2. Complete the proper testing for all Releases into the managed environments
3. Assign individuals to participate in the Release and Deployment Management Process, and represent the IN.gov Web Portal;
4. Participate in the functions and work activities associated with Release and Deployment Management, including:
   1. Create Release plans and perform tracking and oversight functions to support the plan documenting all aspects;
   2. Coordinate the Design, Build, and Configuration of the Release;
   3. Coordinate Release acceptance activities with IOT;
   4. Develop and implement rollout plan for the Release;
   5. Develop and coordinate Release communications, preparation, and training activities;
   6. Coordinate distribution and installation of Releases; and
   7. Provide updates to IOT management regarding Release status
5. On an ongoing basis, Contractor shall verify that only authorized users are granted access to the IN.gov Web Portal Production Environments in accordance with the Information Security Framework.
   1. **Reporting**

The Contractor is responsible for developing reports in accordance with this Scope of Work and at the request of a specific State Entity User. As part of the Contractor’s reporting duties, the Contractor must utilize Microsoft Project Online to complete the duties outlined in the section, unless otherwise agreed to by the State. All reporting templates that the Contractor utilizes must be standard Microsoft Project Online reporting templates or templates that are otherwise agreed to by the State. The Contractor’s reports shall be driven by data and include detailed, comprehensive analyses, narratives, and/or graphics (e.g., charts, graphics, and tables) where applicable.

* + 1. **Status Reports**

To convey the status of projects and Contractor activities at a high-level, the Contractor must furnish the below status reports.

* + - 1. **Project Status Report**

The Contractor shall provide the State with a Project Status Report, at a cadence to be determined by the State. The report shall provide an update on all planned and active project activity, including a Project Management Report that illustrates:

1. A status update of all projects (inclusive of Baseline Services and additional services outlined in a Scope of Work or a Task Order) by application, including:
   1. Responsible State Entity User (and point of contact)
   2. Contractor’s responsible employee
   3. What phase the project is in
   4. An Action Item list/status update
   5. Brief statements highlighting issues (if any)
   6. Key dates
   7. Major milestones
   8. A risk assignment mitigation plan
   9. A coding of Green, Yellow, or Red to signify the status at a high-level of the project, including an important data point displaying how the project is trending,
   10. status of individual project areas, including schedule, cost, and quality
   11. For projects outside of Baselines Services only: total project hours budgeted compared to project hours delivered, arranged by major milestone
2. A list of documents awaiting signature
3. Justifications for delayed projects
4. A list of potential revenue opportunity projects
5. A creative resource planning report by project
6. A project plan for self-funded projects, including cost and project timeline information
7. An updated organization chart
8. A Gantt chart to illustrate the overall project schedule
   * + 1. **Monthly Performance Report**

Each month, the Contractor shall furnish a monthly performance report or dashboard. This report or dashboard provides an overall picture of application development projects and status, along with the applicable SLA performance, financial reporting and data sales statistics, and select Web Portal statistics. The report shall be in alignment with and/or contain all of the information that is found in the dashboard at this link: https://www.in.gov/inwp/about-us/metrics/. The Monthly Performance Report is due within the first five – seven business days after the start of the following month. This report is publicly posted on the State’s website.

The Contractor shall also develop project-specific dashboards to State Entity Users that contain key metrics relating to project status, at no additional cost to the State.

* + 1. **Management Reports**
       1. **Monthly Late Log Report**

The Contractor shall maintain for all active projects a Late Log Report, updated weekly, with a summary of missed milestones for the week and the reasons for missed dates.

* + - 1. **Project Staging Report**

The Contractor shall furnish a project staging report that contains all small non-complex projects that take less than 6 weeks. It also contains a report of the initial engagement(s) with the State Entity User to start formalizing an initial Project Charter, Task Order or Statement of Work.

* + - 1. **Additional Management Reports**

The Contractor shall submit Web Activity Reports, to capture web site use analytics and third-party portal managed application usage, at the direction of the State.

The Contractor shall furnish a report detailing their performance against all Service Level Agreements listed in RFP Attachment L- SLAs. The Service Level Agreement report shall be delivered no later than seven days after the start of the following month.

The Contractor shall develop ad hoc or custom reports at the request of the State. Deadlines for ad hoc reports shall be determined by the State according to a scale of urgency.

1. Type 1: 24 business hours turnaround time
2. Type 2: Two (2) business days turnaround time
3. Type 3: Five (5) business days turnaround time

The State and the Contractor shall together make the determination as to whether a report is a Type 1, 2, or 3 report.

* + 1. **Financial Reports**

The Contractor shall be responsible for furnishing Financial Reports (including monthly invoice reports and annual audited financial report of the Contractor).

The Monthly Financial Report shall include, at a minimum, detail on subscribers, State Entity User name, service code and name of service, State Entity User net, user fees, Contractor gross revenue refunds, returns, hosting, and task order charges and shall be in the format approved by the State. The Contractor shall prepare a quarterly report of IOT gross revenue by State Entity User and by service code, which shall be a summary and compilation of those aspects of the Monthly Financial Report.

* + 1. **IN.gov Security and Privacy Reports**

The Contractor must provide the following types of reports to validate adherence to all appropriate security and privacy measures and demonstrate the “health” of the IN.gov environment.

Reports include:

1. An updated asset list to be reviewed yearly with the State
2. Results of security controls and policies audit to be delivered at a frequency to be determined by the State
3. Quarterly PCI reports
4. Results of web application vulnerability scans to be delivered at a frequency to be determined by the State
5. Monthly Potential Threat Assessment and Mitigation Recommendations
   * 1. **Web Content Management Reports**

The Contractor must provide or make available the following web content management logs/reports:

* 1. Web server requests: All requests to IN.gov Web servers, whether application software or otherwise (including errors), are logged and archived per a back-up and retention schedule created by Contractor.
  2. Web application requests: Critical IN.gov application software shall generate individual archive logs of every Web request, with the exception of personal information fields such as social security numbers, dates of birth, credit card numbers, credit card expiration dates and banking information.

These requests must be retained for a minimum of 12 months by the Contractor.

The following are typical reports used to track the operations and performance factors of the IN.gov Portal. The State may add additional reports as needed. The Contractor shall be responsible for furnishing these reports, unless otherwise specified by the State:

1. Incident Reports
2. Current Escalation lists
3. Production Problem Response
4. IN.gov Availability reports
5. Scheduled Maintenance
6. Application Reliability of Existing and New IN.gov services
7. Support Queue
8. Infrastructure performance
9. Help Desk customer call answer time data
10. Routine performance monitoring of the IN.gov Infrastructure
11. Alert notification capability for components of the IN.gov Infrastructure
12. Graphs and statistics to measure usage of the IN.gov Infrastructure
13. Load balancing with SSL acceleration for services deployed on the IN.gov Infrastructure
14. Provide State access to a content publishing system (FTP access)
15. Provide routine traffic analysis and packet logging through a network intrusion detection (e.g., Snort) for the IN.gov Infrastructure
16. Network name services for secondary DNS
    * 1. **Reporting Functionality**

The Contractor's Baseline Services staff shall be responsible for creating user accounts, using the States Single Sign On solution, for State Entity Users to view the information and reports as provided by the Contractor. The Contractor shall grant authorization to the State as "users", as necessary, to facilitate "read" access to reports provided within the Contractor’s reporting software.

* 1. **Service Level Agreements (SLA) Overview**

Service Level Agreements for the Contract resulting from this RFP are outlined in RFP Attachment L-SLAs. The Contractor shall meet or exceed all Service Level Agreements and also monitor and maintain their performance in regard to the SLAs each month, both independently and with third party verification tools. The Contractor shall furnish a report detailing their performance against all Service Level Agreements that shall be delivered no later than seven days after the start of the following month. For more information regarding SLA reporting requirements and SLA details, please see Section 1.5.2.3- Additional Management Reports of this Scope of Work and RFP Attachment L- SLAs.

The details of the SLAs may be modified during the term of the Contract. An executive SLA performance review with the State is required every 6 months. SLA performance is a key input during contract renewal.

**1.6.1 SLA Liquidated Damages**

The Service Level Agreements will have associated liquidated damages for failure to meet the standards, which will be determined during contract negotiations. Imposition of liquidated damages is discretionary. The State will discuss and give the Contractor the opportunity to respond to performance standard issues, and may waive, give the Contractor the opportunity to earn back, or reduce the liquidated damage based on circumstances of a particular performance standard failure. Liquidated damages will be capped at 10% of the total Baseline Services cost.

If assessed, the Contractor may be given the opportunity (at the State’s sole discretion) to earn back the liquidated damage amount. If the State chooses to allow the Contractor to earn back the liquidated damage, the Contractor must meet the metric in the following two reporting periods in order to earn back the liquidated damage. If achieved, the Contractor must receive verification from the State and submit a claim to have the associated liquidated damage amount returned. If the Contractor does not meet the metric in the following two reporting periods, the Contractor may not earn back the liquidated damage amount.

* 1. **Training**

The Contractor shall be responsible for leading or assisting the State with the training activities as outlined below:

1. Provide staffing necessary to train State Entity Users in Third-Party Portal Managed Applications on an as needed basis. For Political Subdivisions this training offering within Baseline Services pricing is limited to the list outlined in RFP Section 1.2.3.1 item 4.
2. Provide staffing necessary to train State 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.
   1. Training options, including one-on-one, group training, and on-line tutorials should be made available in order to best meet the needs of State Agency users. The Contractor shall provide the State with written training materials, including templates / guides of best practices and commonly-used code, that State Agency users can independently reference.
3. Conduct web content management user training for all content managers and communicators. State Agency Users receive Web Accessibility and SEO training. This enhanced offering should be available to Political Subdivision users through a Task Order.
4. Conduct an annual security training program for all content managers including documentation/training on how to use the platform in a secure manner.
5. Develop and maintain user, provider, and operations manuals
6. Perform and/or enable baseline staff to attend or participate in applicable Web Portal-related trainings.
   1. 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 Contractor shall develop and maintain a robust Training Plan that illustrates how they will meet the above numbered requirements. The Training Plan shall also outline the Contractor’s overall training strategy and techniques. The Training Plan must include: key objectives, how they will meet the requirements listed in the bullets above, training tools, roles and responsibilities, training environments, approach and methodology, training types, materials, and effectiveness.

The Contractor must provide a sufficient number of staff to successfully accomplish all of the requirements of the Training Plan and all requirements listed in the numbered bullets above. The Contractor’s training group must have proven experience in the development and delivery of comprehensive training for a project of similar scope and scale.

At any time, IOT may identify new or improved tools to be included as part of the Web Portal services. In these cases, the Contractor shall be responsible for developing and delivering trainings on these tools, unless otherwise specified by the State.

Additional training requirements related to the transition of services can be found in Sections 1.19 and 1.20 of this Scope of Work.

* 1. **Help Desk and Customer Support**

The Contractor shall provide Tier 1 technical support for the application software and web pages developed by Contractor ("Supported Services") to State Entity users and customer support for public users, Monday through Friday from 8:00 AM to 5:00 PM Eastern time, excluding State holidays and weekends ("Help Desk Hours"). Contractor shall provide 24/7 technical support for all Tier 2 responsibilities as determined by the State.

All help desk support shall be provided by live customer service representatives available by toll-free telephone and shall be located in the United States. The Contractor must 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.

Help Desk Support issues, as submitted through the Webmasters website (for more information, see Section 1.4- Project Management, Change Management and Release Control) or by phone, include but are not limited to:

1. Non-availability of static web content
2. Application non-availability
3. Response time problems

The Contractor shall also provide help desk services related to change management issues and incidences.

The Contractor shall use the State's help desk solution software for managing content changes. All content changes will be handled by priority level and every request for a content change shall be logged through the State's help desk, which will serve as the State assignment of the content change to the Contractor. Prior approval of IOT is not required to proceed with content changes. See Section 1.12.5- Content Changes for additional details.

Help Desk tickets and inquiries shall be assigned Tiers. The Contractor’s Help Desk shall respond to Tier 1 inquiries. Requests for technical or customer support that are received by the Contractor personnel and which pertain to other State applications or State system issues shall be forwarded to the State for referral to the appropriate third-party vendor or State personnel.

The Contractor shall respond to Tier 2 security and privacy inquiries, or other Tier 2 inquiries as determined by the State.

* 1. **Marketing**

The Contractor shall serve as a marketing arm of IOT in marketing the IN.gov web design, application development, and portal services. The Contractor must proactively market and promote to State Entities the benefits and use of IN.gov Web Portal services as part of an overall State Entity User Technology Needs Assessment and Support review as outlined in RFP Section 1.2.2.4 State Entity User Technology Needs and Support.

In addition, the Contractor shall develop a Marketing and Outreach Plan, when requested, to include the approach for outreach and marketing and approach to reaching a broader customer / user base (e.g., Political Subdivisions).

In connection with its marketing responsibilities, the Contractor shall:

1. Use the IOT-approved change management process for all platform and tools used to support marketing changes
2. Aggregate web analytics data to gain insights and provide feedback into marketing strategies
3. Actively market its development services and seek out opportunities to increase the functionality of the IN.gov Web Portal
4. Build and maintain active relationships with nationally-recognized groups, such as, organizations like the National Association of State Chief Information Officers (NASCIO), the American Association of Motor Vehicle Administrators (AAMVA), the National Association of Secretaries of State (NASS), the Center for Digital Government (CDG) and the World Wide Web Consortium (W3C)

**1.10 Invoicing**

The Contractor shall submit an invoice to the State requesting payment of the Baseline Services on a monthly basis. The invoice shall contain any specific detail required under a relevant Scope of Work. The invoice shall be submitted in conformance with State guidelines and requirements regarding format, manner and time of submission invoices. The date of submission for the invoice shall be the same date each month as agreed to by the parties.

The Contractor shall submit an invoice for any Time and Materials Services performed pursuant to a signed Task Order or Change Order. The invoices shall contain the specific details required under the applicable Task Order or Change Order, and shall be submitted at the interval indicated in the applicable Statement of Work, Task Order or Change Order, or, if no interval is specified, monthly at the time the invoice for Baseline Services is submitted. The invoice shall be submitted in conformance with State guidelines and requirements regarding format, manner, and time of submission invoices. The date of submission for the invoice shall be the same date each month as agreed to by the parties.

As part of the Baseline Services, the Contractor's staff shall prepare a monthly invoice for services used on IN.gov. The form of the invoice shall be approved by the State, such approval not to be unreasonably withheld, and shall be sent to the customer's billing contact either online or by mail. The Contractor shall develop and implement procedures to utilize electronic invoices, which procedures shall be approved by the State, such approval not to be unreasonably withheld. Per-transaction charges shall be in accordance with the then-current IN.gov account agreement and applicable service schedules, and shall be subject to applicable sales and use taxes, which taxes may be charged by the Contractor in addition to the agreed-to per-transaction charges. Terms of invoice, payment shall be net thirty (30) days. IOT shall be responsible for disbursement to the proper State Entity User accounts based on the reports and invoices generated by the Contractor.

The Contractor is also responsible for maintaining a database of all transactions processed for the month, by entity, and invoicing customers on a monthly basis, with electronic invoices the preferred billing method.

The Contractor shall submit a Monthly Finance Report that accompanies each monthly invoice that provides a line-item breakdown of all Contract costs. For more information regarding Monthly Finance Reports, please see Section 1.5.3 Financial Reports.

**1.10.1 Non-Electronic Payments from Users**

The Contractor will provide monthly account users who do not pay electronically with a monthly invoice either online or by US mail. The Contractor will establish a lock box to receive all paper payments of monthly account invoices. The Contractor is responsible for all fees associated with lock box account maintenance and support.

All monthly account paper check payment funds must be deposited to the State-designated bank account via a lockbox. The lock box service provider is responsible for depositing the contents of the lock box in the bank designated by the State. The State uses the Account Database or System (as outlined in Section 1.17.1 Account Database or System) maintained by the Contractor, the Lock Box report and the corresponding Bank Deposit receipt to reconcile payments. The Contractor is not an active party to the deposit and disbursement of the funds to the State and is not responsible for the amount or for the schedule of deposits to the State from the paper check users.

* 1. **Security**

Security of the IN.gov Web Portal and protection of non-public information transmitted through and over the portal is of paramount importance to the State. The following terms and conditions apply to all services provided by the Contractor on behalf of the State, whether a Baseline Service or Time & Materials, and whether data is housed at the Data Center or elsewhere.

* + 1. **Background**

Security is defined as “protection against unauthorized access to, or alteration of, information and system resources, including CPUs, storage devices and programs” or “the state of being free from danger or threat.” In an effort to continue to provide optimum security protection for all systems and applications that support the IN.gov Web Portal, the Contractor must provide support staff as part of Baseline Services for three critical areas:

* Security
* Privacy
* Compliance with any/all Federal, State and other laws, rules and regulations

The security and privacy staff assigned to this program area shall provide comprehensive, day-to-day operational security and privacy support for the three hundred plus (300+) websites and growing, securing infrastructure components that process over ten (10) million financial transactions annually, and the application software that is developed and maintained for the State and in production on IN.gov.

Security and Privacy includes:

* Compliance to all standards governing data security and includes data entry, storage, access, backups, and transaction logging and reporting
* Security Policy
* Privacy Policy
* Security Awareness Program
* Privacy Program
* Privacy Awareness Program
* Security Architecture
* Privacy Architecture
* Disaster Recovery/Business Recovery/Business Continuity Plans
* Management of PCI DSS requirements, PHI and Personally Identifiable Information (PII) protection requirements

The IN.gov Web Portal crosses all branches of State government with approximately 110 agencies. The Contractor supports over 300 public-facing websites and close to 1,000 domains and growing. Over 90% of the 300+ websites are in the State Web Content Management System. There are over 125 applications within the IN.gov Web Portal, many of which contain PII and/or provide payment processing and require a higher level of security.

* + 1. **Compliance with Established Standards**

At a minimum, the Contractor shall comply with the following:

1. State's most current Information Security Framework, which is based on the National Institute of Standards and Technology standards (NIST.gov).
2. Maintain an on-going security enterprise certification based on NIST standards
3. Provide a Certificate of Cyber Insurance, annually
4. The Contractor shall comply with the State's Cloud Product and Service Standard ID: IOT­ CS-SEC-010.
5. The Contractor shall, as applicable and at its sole expense, comply with the following industry standard best practices unless otherwise agreed to by the parties:
   1. The latest versions of NIST SP 800-53 and 800-53A for data in use, in transit, and at rest.
   2. The latest versions of NIST SP 800-53A, NIST SP 800-30, NIST SP 800-37, NIST SP 800-115
   3. The latest version of CSIS 20 Critical Security Controls
   4. Payment Card Industry Data Security Standard ("PCI DSS"), and shall provide an Attestation of Compliance upon request (if applicable)
   5. NACHA Operating Rules (if applicable)
   6. SOX Security Compliance
   7. Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines (WCAG) 2.0
   8. The latest version of the Indiana Office of Technology’s TLS standards and requirements
      1. **Third Party Enterprise Agreement**

The Contractor shall maintain an Enterprise Security Assessment or a similar third-party assessment, and shall annually provide the State with evidence of such assessment. When requested by the State, the Contractor shall make available risk assessments performed in conjunction with this section for review by the State. The Contractor shall select another similar third-party assessment offered by a nationally recognized firm, if available, or Contractor shall retain another third-party security company of its choice to perform a comprehensive security audit in connection with the services being performed by Contractor under this Contract. The Contractor shall remediate any deficiencies found by the third-party security assessor based upon a mutually-agreeable risk scoring standard, such as the Common Vulnerability Scoring System (“CVSS”), to ensure that changes are implemented in a timely manner for known vulnerabilities. The Contractor must keep their reports in line with SOC 2 Type 2 standards. Any risk assessments or security audits performed in connection with this Section shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b) (10), (11) and (19).

* + 1. **Security, Risk Monitoring, and Assessments**

All documents associated with the following subparagraphs shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b)(10), (11) and (19).

* 1. The Contractor shall maintain a formal, defense-in-depth Security Incident Response Plan, which shall describe how the Contractor will respond to security incidents and shall also describe the security strategy that will be used to provide ongoing security for State resources in the Contractor’s environment. The Security Incident Response Plan shall be updated on an ongoing basis, with updated copies provided to the State. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor’s environment.
  2. The Contractor must complete and deliver a formal security risk self-assessment of the Contractor’s environment, with a strategy and action plan to address identified risks. Updates to the assessment must be delivered to and reviewed with State security staff quarterly until all identified risks are resolved.
  3. The Contractor, using its own staff or a subcontractor, shall provide an internal security auditor, who is PCI DSS certified, to consult with the State on PCI DSS and security matters in relation to the Contractor’s payment processing program.
  4. The Contractor shall utilize a security testing approach that aligns with NIST 800-115, Technical Guide to Information Security Testing and Assessment.
  5. The Contractor shall provide continuous monitoring, based on applicable NIST 800-137 guidance, of the technical environment(s) that house State applications. The Contractor shall conduct comprehensive manual and automated reporting on a regular basis, the results of which must be provided to the State at least monthly, and on demand by the State when necessary.
  6. The Contractor shall complete an appropriate PCI DSS Self-Assessment Questionnaire on an annual basis, shall conduct quarterly network vulnerability scans conducted in accordance with PCI DSS requirements, and shall annually conduct application penetration testing with a third party on applications developed by the Contractor that accept PII, PHI, or payment processing information within the application.
  7. The Contractor shall continuously monitor and, to the extent it receives information specific to the State of Indiana, provide to the State real-time, up-to-the-minute threat intelligence to include strategic (through recognized national and global security sources) and tactical and operational/technical intelligence. Any changes to the threat landscape that could reasonably and materially impact the State must be communicated in writing and include advice on action to be taken by the State if required.
  8. The Contractor shall employ the Intrusion Detection Systems and Intrusion Prevention Systems, which will be supported with current technology.
  9. Contractor must participate in quarterly meetings with designated State security staff to provide security activity updates. These updates must be compiled in line with SOC 2 Type 2 standards.
  10. Any third party engaged by the Contractor to perform security testing, monitoring, or external network vulnerability assessments shall be approved, in advance and in writing, by the State. The Contractor shall remediate any deficiencies found by any third-party security assessor based on a mutually-agreeable risk scoring standard, such as CVSS, to ensure that changes are implemented in a timely manner for known vulnerabilities.
      1. **Disaster Recovery and Business Continuity**

The Contractor shall maintain and share with the State a Disaster Recovery Plan, and shall make available to the State all amendments, changes, or modifications to its Disaster Recovery Plan, which is deemed a trade secret and is deemed information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana’s Access to Public Records Act, Ind. Code § 5-14-3-4(a) and (b)(10), (11) and (19). This is in addition to, but may include, the Disaster Recovery Plan required for the Data Center. The Contractor shall, in coordination with the State, maintain a specific Business Continuity Plan dedicated to operating State systems for which it is responsible in the event of a disaster.

**1.11.6 Security Plan**

1. The Contractor shall have in place a comprehensive Security Plan and Internal Control Plan.
2. The Contractor must provide a formal, defense-in-depth security strategy, 30 days from contract execution, that will be used to provide ongoing security for State resources in the Contractor environment, update the strategy on an ongoing basis, and inform the State in writing within thirty days of strategy updates. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor environment.
3. The Contractor must utilize a security testing approach that aligns with NIST 800-115, Technical Guide to Information Security Testing and Assessment.
   * 1. **Audit Controls**

The Contractor shall obtain and provide a copy of the annual independent audit of the Data Center(s) at its expense and shall, upon completion, provide an un-redacted version of the complete audit report to the State. A Service Organization Control (SOC) 2 audit report or equivalent approved by IOT sets the minimum level of a third-party audit. The State may also perform an annual audit of the Contractor’s collocated space within its Data Center(s). The audit may take place onsite or remotely, at the State’s discretion. The State shall provide to contractor thirty (30) days’ advance notice prior to the audit. The Contractor shall make reasonable efforts to facilitate the audit and shall make available to the State members of its staff during the audit. The State may contract with a third-party to conduct the audit at its discretion and at the State’s expense. The audits conducted under this paragraph are deemed information that is a trade secret and that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana’s Access to Public Records Act, Ind. Code § 5-14-3-4(a) and (b) (10), (11), and (19).

The Contractor shall provide an audit trail for all transactional and administrative tasks. The Contractor’s portal support must provide the capability to maintain access roles that dictate permissions for system/application access. Roles may be added, updated, or deleted by an Administrator. The Contractor shall store log capture information for a minimum of one year from date of capture. The Contractor shall perform annual internal security audits to help thoroughly test Contractor’s security posture. Audit reports and risk mitigation plans must be made available for review by the State one month after completion, and shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b) (10), (11), and (19).

**1.11.8 User Accounts**

The Contractor shall adhere to applicable NIST standards and best practices governing management of user accounts, such as time-driven auto disablement, account deletion, locking of accounts, and maintenance of user profile data following deletion. User accounts shall be reviewed for inactivity at a quarterly rate at minimum and appropriate action taken; auto disablement, account deletion and/or locking. When possible, the Contractor shall use the State’s SSO to manage user accounts. User accounts must follow IOT password complexity requirements. Accounts with privileged access which are authenticated by the Contractor are required to have at least NIST 800-63 AAL-2 authentication. The Contractor shall provide the capability for password encryption before the password is recorded in any data repository. Passwords shall not be stored directly; rather, a cryptographic hash of the password shall be stored. Password hashing must adhere to NIST 800-63B Section 5.1.1.2.

* + 1. **Software Security Features relating to IN.gov Infrastructure**

In addition to the security requirements imposed on the Data Center above under Section 1.3.1.3.2 Data Center Requirements, the Contractor shall provide, at a minimum, the following software security features for the IN.gov Web Portal:

1. “Stateful” or equivalent inspection firewalls shall be used to help regulate all network traffic from the internet into the DMZ segments and communications between network tiers.
2. Infrastructure that supports a configuration that performs as a DMZ for Contractor-supported State applications.
3. A multi-tier application architecture shall be used to help limit communications between the tiers to mitigate against an intruder from accessing critical systems attached to network segments.
4. VPNs or another means of secure communication agreeable to the State shall be used to help prevent unauthorized internal intercept of communications between IN.gov and State systems.
5. Intrusion detection products shall be used to help identify and report intrusions to the Contractor’s staff so they make take immediate counter-measures.
6. Virus protection software shall be used to help proactively identify computer viruses.
7. Development workstations shall be secured in a commercially reasonable manner to mitigate the risk that an intruder will gain access to the server infrastructure through a compromised workstation.
8. Remote access by portal employees shall utilize VPN client software using multi-factor authentication mechanisms to mitigate the risk of unauthorized remote entry into the system.
9. Identify security incidents which penetrate the IN.gov servers maintained by Contractor and compromise data (defined as obtaining or altering confidential user information, transaction data, or authorized static content), and shall notify the State within two (2) hours of confirmation of the incidents.
10. The Contractor shall maintain and follow a patch management Standard Operating Procedure reasonably acceptable to the State designed to provide a secure network environment for its applications, staff, business partners, and contractors so that all electronic devices (including servers, desktops) connected to IN.gov network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The Contractor shall report any exception to the Standard patching schedules to the State.

**1.11.10** **Protection of Personally Identifiable Information**

“Personally Identifiable Information” in Ind. Code 4-1-11-3. This paragraph supplements the requirements of the Contract relating to confidentiality of State Information, PII, and the Security and Privacy of Health Information. The Contractor shall comply with the following privacy standards (and the State shall require all agencies using IN.gov, and shall require any third-party vendors providing applications to IN.gov, to comply with the same):

1. Not less than IOT’s TLS encryption standards to protect Web requests that contain as applicable:
   1. User credentials (username and password)
   2. Sensitive information (credit/debit cards numbers, checking account and routing numbers) and any forms of user authentication
   3. Personal information as defined by Ind. Code § 4-1-11-3
   4. Personal information as defined by Ind. Code § 24-4.9-10
   5. Highly restricted personal information in a driving record as defined by Ind. Code § 9-14-16
   6. Protected health information as defined by the Health Information Technology for Economic and Clinical Health Act
2. Documenting, for each application, what information will be accessed, how it will be accessed and provided to the public, an assessment of the access method and what, if any, special authentication requirements must be satisfied by the individual customers to qualify for access. Such documents are deemed information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana’s Access to Public Records Act, Ind. Code § 5-14-3-4.
3. The Contractor shall ensure that all PII is housed in the continental United States, inclusive of backup data.
4. The Contractor must provide a system that shall encrypt all financial and confidential data transmissions.
5. The Contractor’s protection of all data retained by Contractor from IN.gov users shall adhere to current Contractor and IOT-specified security policies in effect at the time of deployment of the application. The service shall also comply with the then-current applicable privacy policies established by the State or the applicable State Entity User, and state, and/or federal law. In the event a change to the State’s or an State Entity User’s privacy laws and/or security policies results in increased Contractor costs, the Contractor shall notify the State of the cost associated with compliance, and the State shall bear the increase. In connection with any services being provided to agencies under Statements of Work or Task Orders, the State Entity User must inform the Contractor promptly of relevant changes in the privacy laws and/or security policies that impact the services being provided by the Contractor.
6. Upon State request, the Contractor shall provide a copy of all PII it holds. The Contractor shall provide such data on media and in a format determined by the State.
7. Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all PII it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology (“NIST”) Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.
8. All data movement within or out of the State environment must utilize an approved State provided process.

**1.11.11** **Privacy**

In addition to the protection of Personally Identifiable Information, the Contractor shall protect the privacy of users and information as follows:

1. The Contractor shall have a written Privacy Program which reflects commercially reasonable practices for privacy programs and incorporates the use of privacy-by-design techniques, including using data de-identification tools for adequate PII and PHI protection when required. The Privacy Program shall be updated as needed by the Contractor and approved by IOT. The Privacy Program is subject to annual review by IOT. The Contractor and IOT shall work in good faith to develop a plan to address the concerns of IOT.
2. The Contractor shall designate a single point of contact (“SPOC”) for all privacy matters. The SPOC shall be familiar with HIPAA and HITECH and the Contractor shall also have a resource with a CIPP/US certification.
3. The Contractor shall have controlled user access, restricting access to all PHI and PII to those staff members with a job-related need for access.
4. The Contractor shall complete Privacy Impact Assessments in a form mutually acceptable to the State and the Contractor, such assessments may use the decision tool used by U.S. Department of Homeland Security to identify and mitigate privacy risks on all re-developed and newly-developed systems and applications that house PII and shall complete a Privacy Self-Assessment for locations under the control of the Contractor that house systems and applications supporting the IN.gov portal.
5. The Contractor shall 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.
6. The Contractor shall assist the State in its compliance with Ind. Code § 4-1-6 as it applies to the Contractor’s systems that collect PII. This includes, but is not limited to, data regulated by HIPPA and FTI.
7. If the Contractor handles federal tax information (“FTI” – defined in IRS Publication 1075, §1.4 [November 2021]) the Contractor must comply with applicable NIST and IRS Publication 1075 security controls and requirements to which the State subscribes. As an example, if the Contractor handles FTI for the Department of Revenue, then the Contractor must comply with all applicable aspects of the NIST 800-53 pertaining to safeguarding such data.
8. The Contractor must ensure that all data is housed in the continental United States.

**1.11.12 Disclosure of a Security Breach**

Ind. Code § 4-1-11 is applicable to the breach of the security of a system that houses information maintained by a State Entity User. If such a breach occurs and involves information in the possession of the Contractor, the Contractor shall fully comply with the notification and reporting requirements of that statute. The Contractor’s performance under this Contract is governed by, among other things, Ind. Code § 24-4.9. The contractor shall comply fully with Ind. Code § 24-4.9, and shall:

1. Notify IOT as soon as it discovers that there has been a breach of the security of data as defined by Ind. Code §24-4.9 (an “Incident”).
2. Notify IOT and the Indiana Attorney General to the extent required by the Ind. Code § 24.9-3-1 within two (2) hours of the confirmation of an Incident. To the extent possible, the parties will follow a mutually-developed Communications Plan and Incident Report detailing the Incidents covered and the reporting and notification requirements under Indiana statute; such reporting and notification may include information specifically identified as confidential or trade secret by the Contractor.
3. Implement and maintain procedures consistent with the requirements of this Contract, including taking commercially reasonable steps to protect and safeguard from unlawful use or disclosure of all Personal Information that is collected and maintained by the Contractor under this Contract.
4. Notify IOT, and the affected persons as required, of any Incident caused by the Contractor’s breach of the requirements of this Section where unencrypted personal information was, or is reasonably suspected to have been, acquired by an unauthorized person through the Contractor’s systems, or encrypted personal information was or may have been acquired through the Contractor’s systems by an unauthorized person with access to the encryption key. However, the Contractor may delay providing notice to the affected persons (1) when the delay is necessary (a) to restore the integrity of the computer system or (b) necessary to discover the scope of the breach; or (2) at the request of the Indiana Attorney General or any law enforcement agency if the disclosure will (a) impede a criminal or civil investigation; or (b) jeopardize national security. The notification to the affected persons delayed under (1) shall be made as soon as the delay is no longer necessary to restore the integrity of the computer system, or to discover the scope of the breach. The notification to the affected persons delayed under (2) shall be made as soon as the Indiana Attorney General or the law enforcement agency notifies the Contractor that disclosure will no longer impede an investigation or jeopardize national security.
5. Notification to affected persons of an Incident caused by the Contractor’s actions or lack of action shall be made by the Contractor at the Contractor’s expense and shall comply with the notification requirements of this Contract and applicable law. Additional remedies, such as making available to the affected persons credit monitoring and call center support shall be conducted as required by law, or otherwise as mutually agreed by the parties.
6. The Contractor shall pay all final judgements, and reasonable attorney fees, and associated court costs due to an Incident that is directly attributable to the Contractor’s actions or lack of action.
   1. **Websites** 
      1. **Website Staffing**

The Contractor shall provide a Creative Services team that includes a dedicated Senior Creative Manager with experience using UI/UX design. The design team is responsible for website redesign projects and professional graphic design, custom HTML, JavaScript, and CSS assistance.

* + 1. **Website Design Standards**

The Contractor is responsible for establishing, maintaining, and updating website design standards to promote a consistent experience across websites and applications. The Contractor is responsible for the implementation of new web sites as requested by State Entity Users in accordance with the standard IN.gov look and feel. These standards shall include at a minimum:

1. An Application Style Guide
2. A standard application header
3. A Web Design Standards and Requirements Document
4. Code reusability
5. User experience tools that are intuitive, accessible to all levels of technical expertise, and promote quick deployment of websites, applications, and standards

**1.12.3 Website Design Tasks**

The Contractor is responsible for the following web design tasks which can be found at https://www.in.gov/inwp/:

* 1. Content changes - which must be handled on a priority level
  2. Graphical element design
  3. Creation of prototype templates as part of the development process
  4. Consistent application look and feel
  5. Application prototyping
  6. Application landing page design
  7. Compliance with § 508 of the Rehabilitation Act of 1973 (Accessibility Standards) with Level A (must support) and Level AA (should support) Success Criteria as defined under Web Content Accessibility Guidelines (WCAG) 2.0, in each case with respect to public-facing portions of the systems. See RFP Attachment-K Assistive Technology Compliance Evaluation Form.
  8. Billboard creation
  9. Web 2.0 Social Media Requests for Social Media tools including, Twitter, Facebook, YouTube, Blogging, and RSS Feeds
  10. Web CMS maintenance in accordance with the current IN.gov look and feel
  11. Conduct frequent user experience testing sessions on website templates and applications

The Contractor shall integrate all IN.gov web technologies in new websites and applications as part of the base design or template inclusive of any advanced features and integrations.

In connection with its web design and marketing responsibilities the Contractor shall:

1. Use the IOT-approved change management process for all platform and tools used to support web design and marketing changes
2. Monitor and process all web content-related requests logged through the IOT Webmasters solution
3. Maintain a response time of at least 200 milliseconds but no more than 1 second for all web pages and report response time on a monthly basis against this Metric
4. Aggregate web analytics data to gain insights and provide feedback into marketing strategies
5. Actively market its development services to the agencies and seek out opportunities to increase the functionality and self-service features of IN.gov
6. Provide § 508 Accessibility Compliance Reports via industry standard accessibility tools as directed by IOT

**1.12.4 Procedural Requirements**

Web design services shall be provided by the Contractor, including development of templates used by IN.gov customers, as a part of Baseline Services. Agencies shall make requests through the Webmasters system as a part of Baseline Services.

Agencies shall have the ability to request assistance with maintaining non-interactive portions of their web presence through an online request via the [Webmasters](http://webmasters.in.govwebmasters) Platform. This shall include such things as HTML, HTML5, JavaScript, CSS, CSS3, graphics, images, and simple email contact forms. The standard turnaround time for these requests shall be three business days.

**1.12.5 Content Changes**

All content changes will be handled by priority level. The Contractor shall use the State's help desk solution software (presently ASM) for managing content changes. Every request for a content change shall be logged through the State's help desk, which will serve as the State assignment of the content change to the Contractor. Prior approval of IOT is not required to proceed with content changes.

Priority levels are defined as:

* High: Requires immediate changes
* Medium: Requires changes within a 2–3-day timeframe
* Low: Work that has a due date in excess of 3 days

**1.12.6 Continuity of Services**

If the Contractor has a maintenance issue that causes services to be unavailable, including the IN.gov static website, the Contractor shall provide a static page that links to high profile services not hosted by the Contractor.

**1.12.6.1 Back-Up Copy**

The Contractor must provide an annual back-up copy of the IN.gov website to meet the State’s record retention policy. The back-up must be in a format acceptable to the Indiana Archives and Records Administration (IARA).

**1.12.7**  **Web Technology Integration and Support**

The IN.gov Web Portal strategically leverages their enterprise-wide platform to negotiate and integrate products and services that benefit the entire IN.gov Web Portal. These services promote a strong web portal presence, § 508 compliance, and ensure the security and integrity of the IN.gov Web Portal. Contractor shall be responsible for providing, monitoring and maintaining resources in support of the following services:

Services available on IN.gov ( <https://www.in.gov/inwp/>) include but are not limited to:

* [Assistive](http://www.texthelp.comassistive) technology
* Online Calendar
* FAQ/Live Chat
* Web-based email subscription management system
* Mobile Application Solutions
* [Content](http://www.siteimprove.comcontent) experience and marketing performance tools
* [Workplace](http://www.formstack.comworkplace) productivity tools
* Map[s](http://www.esri.coms) for websites and applications
* Search Appliance
* Stock imagery resource

As part of Baseline Services, the Contractor shall keep all IN.gov-supported and hosted, third-party, portal service applications current, shall monitor release announcements, perform software updates on a timely basis following the State’s notification protocol, coordinate with IOT in defining third-party application hosting standards, and must maintain version control history and documentation for all IN.gov supported, third-party portal service applications as outlined in Section 1.16 Third-Party Applications.

**1.12.8**  **Website Domains**

As part of Baseline Services, the Contractor shall be responsible for the management of the current 300+ public and internal facing websites and 1000 domains and the subsequent addition of websites and domains in support of the ongoing Web Portal growth. Exhibit 2- Current Website List includes a listing of all current websites.

This includes:

1. The State’s current .gov domain names: IN.gov, myin.gov, Indiana.gov, myindiana.gov, ourindiana.gov
2. Domain name purchases and all subsequent renewals
3. Management and maintenance of the current portfolio of 1000 domains

**1.12.8.1 Vanity URL’s**

Contractor shall manage and maintain all vanity URLs and provide a process by which State Entities can determine the active status of each URL at renewal points. RFP Exhibit 3- Vanity URLs includes a listing of current Vanity URLs.

Any State entity on the IN.gov network shall have the ability to request specialty URLs including .com, .net, .org, etc. Review and approval by IOT shall be required for all requested URL’s.

In accordance with IOT policy, all vanity URL (non-IN.gov) domains are subject to a third-party domain registration fee and must be kept indefinitely once purchased. As such, the State would like to optimize registration fees by evaluating costs for various registration periods (1 year, 5 years, 10 years). Contractor shall work with the requesting State Entity User to determine the appropriate registration period for each requested vanity URL. Contractor shall pass through the registration fee to the requesting State Entity User via a Task Order.

The Contractor shall notify IOT and the State Entity User using the vanity domain(s) 90-days before expiration to initiate the renewal process.

**1.12.8.2 Refreshes**

Under the direction of IOT, the Contractor shall design, plan, schedule and then execute a biennial technology refresh of the IN.gov home page, which includes applications, web services, and web integration technology that integrates with home page and are branded with the same header and footer of the IN.gov Home Page.

The Contractor shall continuously look to identify emerging technologies and standards to improve capabilities and increase performance. This research shall include user testing and focus groups. As part of biennial technology refresh, the Contractor shall present the findings of such research with recommendations to the State.

The Contractor shall be responsible for executing a refresh of the IN.gov home page and related non-State Entity pages every other year, at a minimum, and a refresh of State Entity home pages in the alternate year. State Entity websites must conform to the web design standards and layout templates as directed by IOT. The Contractor must then work with each of the agencies to adopt an appropriate template and create a fresh look for presenting State Entity content and links.

The Contractor shall keep IOT informed of new software release schedules as part of the overall technology refresh strategy.

* 1. **Content Management Systems (CMS) Requirements**

**1.13.1 Background and Scope**

Enterprise Web Content Management shall encompass support of the State’s Web Content Management System (WebCMS), overall web technology innovation and implementation, and responsibility for planning and executing the recurrent web technology refresh.

Managing the State’s CMS includes all aspects of the CMS system—maintaining the software, ensuring the web content meets all State web design standards, processing requests for content changes, ensuring the integrity of links, and conducting user training for State content managers and communicators.

The current IN.gov web portal consists of 240,737 htm and html pages. This includes approximately 43,259 pages managed through the current Web Content Management System.

The State’s objectives and goals in using its CMS system are to:

1. Establish a consistent IN.gov brand across IN.gov
2. Reinforce the IN.gov brand, which communicates trust, security, and ease-of-use
3. Reinforce that Indiana's entities are part of a larger state government, while still allowing those entities to communicate their own message
4. Improve usability and accessibility
5. Provide adequate training to all content creators and approvers
6. Establish and maintain CMS environment

**1.13.2 Operational Requirements**

The Contractor shall provide, manage and maintain a Web Content Management System (WebCMS). Currently, the State’s WebCMS is Squiz Matrix Web Site Management. This includes:

1. Maintaining the software
2. Standards as established by the Contractor and approved by the State
3. Processing requests for content changes
4. Ensuring the integrity of links on the Core Website (http://www.in.gov/core)
5. Comply with § 508 for public-facing aspects under the Contractor’s control
6. Conducting user training for State content managers and communicators as mutually agreed in writing
7. Partner with the State in communicating with any WebCMS vendors

The Contractor shall manage content and images purchased by it for use on the IN.gov Web Portal. Contractor must also provide a mechanism for State Entity Users to submit their content and images for management, which may be integrated into the current asset manager using a global asset manager. The State is responsible for any content submitted by a State Agency pursuant to this Section and the Contractor shall not have any liability if such content violates any third-party rights. Political Subdivisions are responsible for any content submitted by them pursuant to this Section and the Contractor shall not have any liability if such content violates any third-party rights.

All websites and applications must incorporate the State’s Enterprise Web Analytics tool as part of the design. The Contractor must design web solutions to be brand-able with data driven configuration, and must provide UI (User Interface) mockups to stakeholders for new user interfaces or changes to existing user interfaces.

All web pages must use the IOT-approved web analytics software. When major design changes, as determined by the State, are made to the portal, Contractor must have an established relationship with a third party to provide analysis and focus group feedback as part of Baseline Services.

**1.14 Innovations and Trends**

**1.14.1 General Innovation**

The State is interested in ways in which the Web Portal can be enhanced throughout the duration of the Contract. The State looks to the Contractor to seek out and recommend innovative solutions for improving the presentation and delivery of e-government services to the populace and for solutions that can create revenue streams for the State government as a way to offset both the cost of technological improvements and the cost of conducting State business. A Contractor that engages in collaborations with other state governments and through related organizations as a way for the State to learn from and share ideas with others is highly desirable.

The Contractor shall recommend innovative solutions (a) for improving the presentation and delivery of e-government services to users, and (b) that create revenue streams for the State government as a way to offset both the cost of technological improvements and the cost of conducting State business. As part of an innovation strategy, the Contractor must seek out and evaluate third-party web solutions to address across-State Entity User needs and present their recommendations annually.

**1.14.2 Technology Innovation**

The Contractor shall assess the current CMS solution, propose an alternative product, and if applicable, complete a proof of concept that will allow the State to determine the viability of the CMS during the performance period. The assessment will be in the form of a formal project that will detail the processes and procedures followed. The deliverables of the assessment may include the following:

1. CMS requirements as defined by the existing software and through interviews with the IN.gov Advisory Council.
2. Analysis of at least 3 leading content management system providers to determine which meet the requirements, as well as any deficiencies.
3. Review and approval of the requirements and analysis by IOT and the IN.gov Advisory Council.
4. In the event that one of the products evaluated is determined to be a viable replacement for the current CMS, and selected by IOT, after consulting with the IN.gov Advisory Council, the Contractor shall work diligently to complete a proof-of-concept using the product selected. Details of the proof-of­ concept shall be defined in mutually agreed to Statement of Work.
5. Upon successful execution of the proof-of-concept, and selection by IOT, the Contractor shall work diligently to assist the State in migrating from the current CMS to the selected product according to the terms in a mutually agreed upon Statement of Work or Task Order.

**1.14.3 Competitions**

On a yearly basis, the Contractor is responsible for identifying relevant national and/or international competitions such as the Government Experience Awards- and submitting the IN.gov website for consideration. IOT has a goal of achieving a 1st place award and is looking to the Contractor to help Indiana stand out as a leader in innovative e-government solutions.

**1.15 Applications**

The Contractor is responsible for the security and integrity of all applications it develops for deployment by the State. In addition to the requirements set forth below, all applications developed by the Contractor shall adhere to the applicable requirements set forth above in RFP Section 1.11- Security. These requirements apply regardless of whether an application is developed as part of the Baseline Services under a Statement of Work, or under a Time & Materials Task Order.

All services and applications, whether developed as part of Baseline Services or as a Time and Materials Task Order, must be supported and maintained by the Contractor as part of the Baseline Services fee.

The Contractor shall ensure that all data-related connections or Application Programming Interfaces (APIs) between entities utilize MuleSoft.

The Contractor must use the State’s Single Sign On Enterprise Authentication standard (SSO) for all applications requiring user sign-in.

**1.15.1 Application Software**

The Contractor is responsible for the security and integrity of all applications developed by it for deployment by the State. The Contractor shall conform to applicable industry practice in its application development. All applications will be developed by Contractor 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. Contractor must build security credentials into each newly-developed application, and shall use application scanning software and a process to promote the release of secure code at the time such code is put into production. The Contractor will use commercially reasonable efforts to implement appropriate changes needed resulting from updates published to the guidelines.

The Contractor shall meet the following standards and requirements for applications developed by it for deployment by the State:

1. Application access to databases must be based on user credentials or service accounts.
2. Applications performing payment processing must do so through an interface with one of the State’s contracted payment processors and the Contractor must meet all applicable and relevant PCI DSS security requirements.
3. The Contractor must complete a comprehensive source code scan (using guidance from SANS, OWASP, and other nationally or internationally recognized sources) of all applications on an annual basis. The Contractor must review the proposed source code scan methodology with designated State security staff members before use of the methodology to complete the source code scan. Upon request, the results must be delivered to and reviewed with the State.
4. The Contractor must use 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.
5. For applications that may involve information having a security classification by the Department of Defense, the State may request the Contractor to consult and follow the Security Technical Implementation Guides ("STIG") from the Defense Information Systems Agency ("DISTA"); the parties will develop an appropriate Statement of Work incorporating the agreed-upon methodology on a case-by­ case basis.
6. The Contractor and the State will identify the appropriate controls to perform from the Information Assurance Support Environment (IASE) STIGs Application Security & Development for all major application changes to existing applications and new application developments where the application contains sensitive data or as requested by the State.
7. As required on a project basis, the Contractor's products and services shall be compliant with Section 508 of the Rehabilitation Act of 1973 ("§ 508"), which shall be documented by internal accessibility policy documents and accessibility testing documentation.
8. As required on a project basis, the Contractor's applications shall use TLS, conforming to IOT’s TLS encryption standards, to protect data containing protected health information as defined in the Health Information Technology for Economic and Clinical Health Act, user credentials, (username and password), credit/debit card numbers, checking account and routing numbers, and personal information as defined by Ind. Code§ 4-1-6-l(b), Ind. Code§ 24-4.9-3, and Ind. Code§ 9-14-13. IOT‘s TLS standard will inform the Contractor as to which versions of TLS are approved, the algorithms and key lengths approved for server authentication, and the algorithms and key lengths approved for session protections.
9. All supported applications must be cross-browser compatible. See IN.gov Supported Browser page at http://www.in.gov/core/browsers.html.

**1.15.2 Application Methodologies, Processes, and Tools**

IOT and IOT State Entity Users maintain and use multiple development methodologies, including Waterfall, Agile, and hybrid Agile. Contractor, IOT and IOT State Entity Users shall discuss and support the appropriate methodology to be utilized with respect to each Application and IOT retains the right to mandate the methodology to be utilized.

**1.15.2.1 Processes and Tools**

Contractor shall:

1. Document and refine application development methodologies for IOT’s review and approval
2. Create methods, processes, and procedures for IOT’s review and approval
3. Coordinate implementation of methods, processes, and procedures
4. Use source control tools to store and manage software builds and releases throughout the software development and maintenance lifecycle

**1.15.3 Application Programming and Development Standards**

The Contractor shall be responsible for the security and integrity of all applications it develops for deployment by the State. The Contractor must:

* 1. Conform to applicable industry practice in its application development. All applications must 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.
  2. Use application scanning software and a process to promote the release of secure code at the time such code is put into production.
  3. Use commercially reasonable efforts to implement appropriate changes needed as a result of updates published to the guidelines.
  4. 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 pre-condition to Contractor compliance.
  5. 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).
  6. Conform to Information Assurance Support Environment (IASE) STIGs Application Security & Development for all major application changes to existing application and new application development devours.

**1.15.4 Application Release Control**

The Contractor shall:

1. Perform all functions required to maintain the current applications environment
2. Perform all application modifications, testing, and acceptance testing needed
3. Assume full responsibility for release packaging and project commitments for the Applications as in the mutually agreed to release procedures
4. Support and adhere to IOT’s process for priority setting, planning, and scheduling of Releases
5. Monitor the release schedule, and report all schedule exceptions to IOT as required by the Change Management and the Release and Deployment Management processes as outlined in RFP Section 1.4 Program Management, Change Management and Release Control.
6. Provide the necessary interfaces during the development, testing and implementation phases.
7. Maintain source code and version control in the Contractor-provided Code Database.
8. Perform malware scanning and eradication on new and modified Software and document the results of such scan and eradication
9. Coordinate the planning and scheduling of all upgrades with IOT
10. Promptly report to IOT any audit compliance issues or e-discovery issues when such issues become known to Contractor

**1.15.5 Application Development Project Initiation**

Application Development projects can be initiated by a State Entity User to the Contractor directly or through the Webmasters.IN.Gov service request system. Projects can also be initiated by IOT. Note: All projects must be approved by IOT before the Contractor engages.

All projects shall follow a process based on the IOT Project Development Life Cycle as outlined in Section 1.4.4.1- Project Development Lifecycle. With State approval, the Contractor may implement its own processes, or modify IOT's processes, to fulfill its obligations to the State.

Application Development shall include the following activities:

* 1. Development Estimation
  2. Application Design
  3. Application Coding
  4. Removed
  5. Cross-boundary Application Development
  6. Cross browser compatibility
  7. Application Maintenance
  8. Unit Testing
  9. Load Testing
  10. Change Orders
  11. Adherence to applicable Standards (State, PHI, PII, Section 508, SOX and PCI DSS)
  12. Requirements gathering and implementation

**1.15.6 Application Repository and Source Code**

As part of Baseline Services, the Contractor must build and maintain an applications and services library where the data is backed by a data store and is manageable online. This library must list all applications used in connection with IN.gov and be designed to grow over time. It shall contain any project portfolio metadata applicable to an application, module or service, such as name, version, where deployed, connection strings, contact persons, description, applicable dashboard pages, and hyperlinks to dependencies when possible. The applications inventory data must be housed via an online database with the backend database hosted at IOT. It must be audited and updated no less than quarterly and readily accessible by the State. The Contractor must work with the State to determine the metadata needed and provide a redesigned Repository within 6 months of a signed Contract.

For each new or updated application, the Contractor must update the applications repository, including key metadata.

All applications must be developed to take advantage of and maximize code reusability, such as for login and Enterprise Service Bus (ESB).

IOT shall maintain ownership of source code and documentation for developed applications. Contractor shall identify reusable source code appropriate for the repository and make available to IOT and IOT State Entity Users in the Contractor provided Code Database.

**1.15.6.1 Application Source Code Security**

Contractor shall:

1. Implement all security requests and password reset requests associated with applications code subject to IOT and State Entity User approval on all data or information requests
2. Install, when required, and maintain source control software in compliance with IOT’s standards and methodology.
3. Monitor and restrict access to source code and IOT Data in accordance with IOT policies
4. Comply with Ad Hoc, annual audit, and regulatory requests
5. Perform IOT Data/source code security audits, and report test results
6. Immediately report any security violations to IOT
7. Promptly report to IOT any SSAE-18 compliance issues or e-discovery issues as such issues become known to Contractor.

Contractor must create a security risk assessment for new and modified applications to identify potential threats and vulnerabilities and proposed prevention measures.

**1.15.6.2 Code Repository**

Contractor shall:

1. Enable and configure a tool to host IN.gov code associated with Developed Materials
2. Develop a method for State Entity Users to obtain and use the available code
3. Create and maintain a list with associated description of available source code
4. Publish updates with newly available code every quarter
5. Prior to code being added to repository Contractor will conduct quality checks to ensure there are no outstanding defects that need to be corrected. The Contractor shall not be responsible for assisting State Entity Users with installation and troubleshooting once the State Entity Users has downloaded the code
6. If Contractor becomes aware of a defect after publishing source code Contractor will correct and republish with a note in the associated description that a new version has been published

**1.15.7 Maintenance of Applications**

All services and applications, whether developed as part of Baseline Services or as a Time & Materials Task Order, must be supported and maintained by the Contractor as part of the Baseline Services. Contractor shall build, execute and maintain plans to successfully and efficiently execute application maintenance procedures. This does not include application enhancements or change orders.

**1.15.7.1 Legacy Application Replacement**

At IOT’s sole discretion and in accordance with the contracted Future Work Rate Card, the Contractor may be tasked with the redevelopment and rewriting of legacy applications associated with the IN.gov program as part of a Future Work order. The Contractor and IOT will identify mutually agreed upon application(s) to be replaced, which shall be identified by a SOW. The SOW will define the work to be done and set forth an anticipated timeline. The Contractor shall track any work under this SOW in the same manner as it tracks other Future Work projects.

**1.16 Third-Party Applications**

**1.16.1 Third-Party Applications – General**

The Contractor shall keep all IN.gov-supported and hosted, third-party, portal service applications current, shall monitor release announcements, perform software updates on a timely basis, adhere to all IOT security and Cloud policies, segment all third-party hosting from the network, and must maintain version control history and documentation for all IN.gov supported, third-party portal service applications.

The Contractor shall provide all necessary third-party applications, unless expressly provided by the State Entity User, their integration and management, as part of Baseline Services, in support of the IN.gov Web Portal. Where Third-Party State Entity User Managed applications are required, the Contractor shall be responsible for the integration as part of Baseline Services. .

Third-Party Portal Managed applications are currently required in support of the following IN.gov functionality:

* Calendar & Events Registration (Localist)
* Accessibility and Quality Assurance (SiteImprove)
* Accessibility Screen Reader (BrowseAloud)
* Automated Web Accessibility Tool (Accessibe)
* URL Shortener (Custom App)
* Content Management System (Squiz Matrix)
* Website Search Tool (FunnelBack)
* Website Analytics (Google Analytics GA4)
* Mapping Development Tool for Web Development (Note: The State’s GIS tool will be the primary tool used for mapping) (MapBox)
* FAQ Solution (Zendesk)
* Chat Bot and Live Chat Solution (Zendesk & Azure Cognitive Services with custom development)
* User Testing (UserTesting.com)
* Web-based Org Chart Solution (PingBoard)
* Form and Workflow Builder and Management Solution (Engagement Builder by Tyler Tech)
* Mobile Application Solutions (MyCivic by Tyler Tech)
* Subscription Service for Website Stickers and Icons (iStock)
* Application Style Guide (Custom Developed – Incumbent)
* Standard Application Header (Custom Developed – Incumbent)
* Training for all Third-Party Applications or First-Party Solutions (Custom Developed – Incumbent)

The State is seeking unique, innovative solutions for all Third-Party Portal Managed applications. Current State details have been provided in Exhibit 7 – Third-Party Portal Managed Tools as a data point only. Respondents are encouraged to propose unique, innovative tools that position the IN.gov Web Portal to remain on the cutting edge of technology and provide the best experience to all users.

Respondents shall consider the following with respect to software ownership and maintenance:

1. Where software is existing and licensed by the State, the State will continue to retain ownership until current software contract expiration, at which time it will be the responsibility of the Contractor to provide the required licenses as part of Baseline Services if such software is determined to be the best proposed solution by the Respondent. Maintenance, in accordance with existing agreements, and management of the software shall be the responsibility of the Contractor until the transition of complete Contractor ownership occurs. During the initial implementation phase, the Contractor shall provide a calendar outlining required license ownership transition. Please see Exhibit 7 – Third-Party Portal Managed Tools for a breakdown of State-owned licenses and current license costs. Respondents are not required to utilize existing software and are encouraged to propose unique solutions that support and advance the IN.gov Web Portal.
2. Where software or future software that is required as a part of the RFP and has not been procured directly by the State, the Contractor must acquire these services as part of Baseline Services. The Contractor shall retain ownership and responsibility for these licenses. During the life of the contract the management and maintenance of the software shall be the responsibility of the Contractor.
3. The State retains all rights to the underlying State data and reports contained in these software elements;
4. As part of a yearly State Entity User Technology Needs Assessment/Support review, the Contractor must look for and identify potential tools and/or technologies that could meet the needs of multiple State Entity Users. As part of Baseline Services, the Contractor shall review with IOT annually and add 3rd Party applications as mutually agreed upon.
5. The Contractor must develop, maintain, execute, and publish a plan to reduce technical debt and increase adoption of service-based capabilities.

**1.16.2 Third-Party Application Hosting**

The Contractor shall provide the following coordination and support activities relating to hosting of third-party applications (those applications developed by someone other than the Contractor or its subcontractors or Affiliates) on the IN.gov Infrastructure as part of Baseline Services for all Third-Party Portal Managed Applications and IOT third-party hosting requirements. All other State Entity User customers shall be given the option of Contractor hosting or IOT hosting for their individual Third-Party State Entity Managed Applications and it shall be entirely at the discretion of individual State Entity Users. In the event an State Entity User elects Contractor hosting, the Contractor shall bill the State Entity User directly using a Task Order and the proposed pricing in RFP Attachment D- Cost Proposal. RFP Exhibit 6- Current Third-Party Hosting Requirements, outlines the Baseline included or State Entity User paid hosting requirements.

Support activities shall be provided for both Third-Party Portal Managed Applications and Third-Party State Entity User Managed Applications. In order to facilitate supporting the third-party applications on the hosting environment, the State agrees to require that third-party application developers develop the application in a way that eases integration, by adhering to IN.gov development and hosting standards promulgated by the State and mutually agreed upon by the Contractor and the State. The Contractor shall not be required to modify third-party software.

In general, the Contractor must follow the procedures identified below to achieve the goal of providing easier support for third-party applications hosted on the IN.gov Infrastructure:

1. The State shall communicate to potential and identified third-party application providers the mutually agreed upon standards for the Contractor hosting platform used to determine whether the application can be hosted on the IN.gov shared platform and how applications interface with IN.gov services, such as payment processing on IN.gov.
2. 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. Baseline testing of third-party applications will be for hosting or enterprise service interface compliance only. More detailed testing or conversion of applications can be performed as part of Baseline Services, as needed. The Contractor will not perform any testing beyond that which is required to determine whether a third-party application appears to meet the published standards for hosting within the Contractor’s hosting environment. Contractor testing does not in any manner make the Contractor responsible for the performance of third-party applications or their affect upon IN.gov once deployed.
3. 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.
4. 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.
5. The Contractor shall not be responsible for the internal functioning of third-party software or its affect upon the portal.

**1.17 Data Management**

The Contractor must develop or provide a system that can manage the data sales and management program for the State (including for both IOT and individual State Agencies like the BMV, ISP, and PLA), including user transactions with the State of Indiana and user accounts associated with those transactions. The Contractor shall also manage applications associated with the data sales system(s) and manage State of Indiana State Entity Users’ access to the system(s).

In executing data management and sales duties under this Contract, the Contractor shall adhere to all relevant State (e.g., IC 4-5-10-1, IC 5-14-3-3.5, IC 9-14-13-7; 9-14-13-8, 9-14-13-9, and 9-14-13-10) and federal (e.g., the Drivers Privacy Protection Act) regulations, statutes, laws, and policies.

**1.17.1 Account Database or System**

As part of the Baseline Services, the Contractor shall maintain an Account Database or System, using the State’s authentication solution, that permits account maintenance, creation, verification, authorization, and invoicing functions. The Contractor shall set up user IDs enabling the State (including both IOT and other State of Indiana State Entity Users) to access the Contractor's database or system.

The Account Database or System shall contain a subscriber center that allow individuals and entities to subscribe to Web Portal premium services. Premium services include but are not limited to:

1. Anytime online access - 7 days per week, 24 hours per day with (the exception of scheduled maintenance or unforeseen outage).
2. Subscriber-only features such as ID Validate, online eFiling for Lobbyists, and Professional License watch
3. The ability to select how you pay - monthly billing or auto-pay
4. Track usage with the ability to view and print statements and invoices

The current IN.gov Subscriber Center can be found at this link: <https://www.in.gov/accounts/home/> and a full list of services can be found at this link: <https://www.in.gov/accounts/ingov-services-price-list/>.

The Account Database or System must 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 authorize users for application use.

The user interface of the Account Database or System shall be responsive with a consistent uniform interface.

The State has adopted a Single Sign On Enterprise Authentication standard (SSO), which will be used to authenticate users and handle certain account maintenance functions such as password resets. The Contractor, at its sole expense, shall expeditiously take the necessary steps so that the Account Database or System is compatible and functional with the State’s solution. The form of the account agreement, user verification requirements, and security and access levels for various applications shall be agreed upon by the State and the Contractor in a Scope of Work. The Contractor may inform the State if it becomes aware of changes or modifications to the account agreements, user verification requirements, or security and access requirements that would improve services offered.

The Contractor shall also collect information from end users, transmit the information to the payment processor or bank, and make certain agreed-to data and information available for review by the State via the Contractor’s reporting tools to support disbursements to the proper State Entity User accounts. As part of the Baseline Services, the State, through the Contractor, shall benefit from any replacements or enhancements to any currently utilized Account Database or System that are generally made available during the term of this Contract. Should the State request IN.gov customizations to the Account Database or System that the Contractor agrees should be incorporated, such customizations will be performed on a Task Order basis.

**1.17.1.1 Account Management**

The Contractor shall be responsible for establishing, verifying, and maintaining user accounts for individuals or entities entering into account agreements for IN.gov. The Contractor shall also manage all subscriptions, including contracts with subscribing entities and third-party contracts related to Account Database or System data.

For reference, there are currently ~5,050 IN.gov subscriber accounts and ~85,427 active users.

The Contractor shall be responsible for the management of these accounts, which includes but is not limited to the following:

1. Account setup and maintenance
   * Account creation, enabling/disabling users, and general user management
2. Generating user IDs and account-related communication to users
3. Ensuring anonymous or unknown accounts are not allowed to gain access to data (e.g., a user with no identifying information cannot access or receive data)
4. Maintenance of hard-copy files containing original, signed data sales user contracts
5. Customer billing questions
6. Credit card expiration date tracking and maintenance
7. Management of government monthly accounts (State Agencies have free access to most portal services, but must maintain a monthly account to capture users obtaining access to services)
8. Implementation of the State's determination of which users should have access to which systems/services
9. Customer service processes to initiate the State's collection efforts for portal monthly accounts, which currently bill in arrears of portal service usage
10. Fielding general user requests from companies, individuals, government agencies, qualifying academic and educational entities pertaining to data sales or the Account Database or System

**1.17.1.2 Access Types**

The Contractor’s Account Database or System must 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 a user.

Access levels that typically are used by individuals and small organizations (e.g., local businesses and local governments) include Guest Access and Subscriber Access. Users with these access levels typically request fewer than 1,000 records each year. For these access levels, the Contractor shall take direct responsibility for the onboarding of users.

*Guest Access:* Guest Access allows users to make purchases without creating an account (note: users still need to provide basic identifying information). For example, an individual can utilize Guest Access to purchase a copy of a driving record. Regardless of whether the user creates an account, the user still must be shown a screen that outlines rules of the data management and sales program and relevant statutes prior to making any purchases.

*Subscriber Access:* Subscriber Access is utilized by individuals and entities that have an IN.gov account and pay recurring fees in addition to per transaction fees. Users with subscriber access have signed an agreement with the State allowing them to access data. Subscriber Access is divided into two sub-group access levels: Basic Subscriber Access and Enhanced Subscriber Access. Basic Subscriber Access allows individuals and entities to access a limited subset of data based on State Entity User-set parameters, while Enhanced Subscriber Access allows individuals and entities to access all data related to a user request. Enhanced Subscriber Access normally requires users to provide verification that they are eligible to receive special access for data related to a user request.

Access levels that are typically used by large organizations include Batch Data Access and Real-Time Data Access. These users typically utilize automated processes to request and receive data. Users with these access levels typically request more than 1,000 records each year. Potential users must be properly vetted and must receive direct approval from the State to be granted these access levels.

*Batch Data Access:* Batch Data Access is leveraged by users seeking to directly receive data on a large scale. Users are sent data via a batch and then periodically receive updates to that data at varying cadences (e.g., weekly, monthly).

*Real-Time Data Access:* Real-Time Data Access is leveraged by users who seek a direct API (utilizing MuleSoft) to State Entity User systems. Changes to data are automatically reflected, so users do not need to rely on period batch updates to view the changes. Some Real-Time Data Access users may seek access to all accessible data in the data management and sales program.

**1.17.1.3 User Authorization Procedures**

When a user submits an application to become an IN.gov subscriber and pays all necessary fees, the Contractor shall grant the user authorization. Depending on the service and access type, the user may then either be granted to access data (e.g., for Basic Subscriber Access) or need to request special access from the State (e.g., for Enhanced Subscriber Access, Batch Data Access, or Real-Time Data Access) to access data.

For authorization levels that require special access, the Contractor must ensure their Account Database or System restricts user access to that data until the special access has been granted by the State. The Contractor must vet users seeking special access to ensure they meet the data management and sales program requirements and present their evaluations and recommendations to the State. The Contractor shall log all research conducted to vet a user and shall, upon request by the State, make available all documents that were factored into an authorization decision. The State is ultimately responsible for communicating which users shall be granted access to data and at what level, based on the Contractor’s recommendations.

Once users are granted authorization, the Contractor shall proactively monitor and evaluate users on an on-going basis to ensure they adhere to all data management and sales program requirements and State and federal regulations. For example, the Contractor will ensure that no user is exploiting the program to retrieve data at a significantly reduced rate compared to other users retrieving that same data.

In the case of employee termination or the requirement that access to the system no longer be granted, the State is responsible for promptly identifying the necessary information to the Contractor.

If a third-party would prefer to have a direct agreement with the State, the third-party will apply for an Account Database or System user ID and execute an agreement with the State (if not already completed). Once executed, the State will then send the agreement to the Contractor. At that point, the Contractor shall permit access to data and manage invoicing (unless otherwise directed by the State).

**1.17.2 Account Database or System Reports**

The Contractor shall develop data sales and management-specific reports for both IOT and State Entity Users. In addition, the Account Database or System shall allow for the viewing of transaction-level detail and reports by State Entity User and/or service.

The Contractor shall submit a quarterly report to the State. This report must contain the following:

1. State Entity User specific breakdowns of data sales
2. Results of quarterly account audits (e.g., a quarterly audit report)
3. New bulk data and subscription requests that will be voted on by the Committee (Note: new bulk data and subscription requests may still be submitted outside of this quarterly report)
4. Other information as directed by the Committee

The Contractor shall also provide data sales information as well as regional/national fee structure information to the Enhanced Data Access Records Committee. For a list of all Account Database or System reports provided currently, please see RFP Exhibit 5- Data Sales Program Reports.

**1.17.3 Data Management and Sales Integrity and Auditing**

The Contractor shall proactively take measures to monitor and ensure the integrity of the data management and sales program. The Contractor must 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.

The Contractor shall proactively monitor for breaches and misuses of data. If a breach or instance of data misuse occurs, the Contractor shall adhere to the Disclosure of a Security Breach Protocol outlined in Section 1.11.12- Disclosure of a Security Breach. The Contractor shall also ensure that all data buyers are held responsible for any breach or misuse of data by themselves or any entity that they sell or distribute data to.

The Account Database or System shall be fully auditable, keeping track of all user actions, transactions, and data pulls, including details on who performed certain actions, when actions occurred, and any dollar amounts associated with the action. Upon request by the State, the Account Database or System shall develop user-specific action logs. The Contractor shall also develop audit tools that can be leveraged by individual agencies when requested.

The Contractor shall comply with all audit requests from the State pertaining to data management and sales. At a minimum, the State will audit account usage in alignment with State statutes and State Entity User requirements (on a quarterly basis) and the Contractor must include the results of this audit in their quarterly report to the State. In addition, the State reserves the right to: directly audit the Contractor with or without advanced notice, directly audit data purchasers with or without advanced notice, require third party auditing, control onboarding criteria for all programs, suspend users who fail to meet program requirements, and suspend users or programs upon an irregularity, such as a data breach.

The Contractor’s Account Database or System must keep track of all defaulted or suspended users. Upon request by the State, the Contractor shall provide a list of all defaulted and suspended users.

**1.17.4 Data Management and Sales Growth and Outreach**

The Contractor shall employ growth strategies to help the State generate additional data management and sales program-related utilization and business. The Contractor shall work with the State to develop State Entity User-specific outreach plans and then manage the implementation of those plans. The Contractor’s plans, strategies, and mechanisms must be clearly defined in the Contractor’s Marketing and Outreach Plan (see Section 1.9 - Marketing for more information regarding this plan).

The State shall have the ability to market via inserts in the materials that will be sent to subscribers.

The Contractor shall aggregate and analyze their growth strategies to understand efficiencies, provide feedback regarding their mechanisms, and drive improvements for future plans. The Contractor shall inform the State of the results of their analysis and future improvements that will be implemented.

**1.17.5 Current State Entity User** **Specifics**

The State of Indiana is permitted under State and federal law to authorize the permissible use of public records. IOT is the entity that manages this process for the State via a subscriber center. Current State Entity User subscriber center services include:

1. Bureau of Motor Vehicles (BMV)
2. BMV Driver License Requests
3. BMV Registration Requests
4. BMV Title Requests
5. BMV Validate Fee
6. BMV Point to Point Drivers’ License Data (PTP DL)
7. BMV Limited Registration Search
8. BMV Digital Certified Drivers’ License Record (DLR)
9. BMV Commercial Drivers’ License (CDL) Driver Monitoring Fee
10. BMV CDL Monitoring Record Pull
11. BMV CDL Driver Monitoring Annual Fee
12. Indiana Department of Child Services (DCS)
13. Child Support Arrears Delinquency Registry (CSADR)
14. Indiana Department of Natural Resources (DNR)
15. DNR Water Permit
16. Indiana Department of Transportation (INDOT)
17. INDOT Miscellaneous Permit Fee
18. Indiana Lobbyist Registration Commission (ILRC)
19. ILRC Employer Lobbyist Registration
20. ILRC Compensated Lobbyist Registration
21. ILRC Activity Filing
22. ILRC Gift Reporting
23. ILRC Amendment
24. ILRC Employer Non-Profit
25. ILRC Employer Compensated Existing
26. ILRC Comp Code Non-Profit
27. ILRC eFiling Late Fee
28. ILRC Compensated Employer Existing
29. ILRC Purchase Report Fees
30. Indiana State Police (ISP)
31. ISP Limited Criminal History
32. Professional Licensing Agency (PLA)
33. PLA License Verification
34. PLA Digital License Verification
35. PLA Bulk Download
36. PLA Bulk Add Records
37. PLA IN License Watch 1 -24
38. PLA IN License Watch 25-100
39. PLA IN License Watch 101-400
40. PLA IN License Watch 401-1200
41. PLA IN License Watch 1201-2000
42. PLA IN License Watch 2000 up
43. Miscellaneous
    * 1. The authorization module is used to provide authorization into various websites (this will eventually be replaced with Access Indiana).

The Contractor shall be responsible for the maintenance of the above subscriber center services. Upon request by a State Entity User and approval by IOT, the Contractor must modify or develop new subscriber center services at no additional cost to the State.

Currently, BMV, ISP, and PLA services comprise the majority of portal-related revenue.

**1.17.6 Invoicing, Fee Handling, and Annual Subscription Fee**

The Contractor shall be responsible for processing monthly invoices and billing all account users each month. The Contractor’s Account Database or System shall aggregate all fees and transactions processed. As part of this aggregation, the Contractor’s Account Database or System must 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 must generate and send invoices electronically.

The State’s payment processing vendor(s) will collect (via online or through the mail) and pass through to the State (via a deposit into the State’s account) any fees associated with subscriber accounts. The account fees are comprised of an annual subscription fee and monthly invoices based on the total number of transactions for each account.

The Contractor’s Account Database or System may have to integrate with the State's payment processing vendor(s) and their system / technologies. The Contractor must be responsible for working with the State’s payment processing vendor(s) 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.

During the term of the Contract, the Contractor will work with the payment processing vendor(s) to ensure the collection (and the pass through to the State) of an annual fee of up to $95.00 to users establishing or renewing an account for IN.gov. Reduction or waiver of this fee for government-funded entities shall be granted upon the State's request and pursuant to applicable law. It is intended to support the monthly account services provided through IN.gov. Any changes to the annual fee will be determined by the State. The Contractor shall be responsible for coordinating with the State’s payment processing vendors to the extent necessary to ensure annual fees are paid and passed through to the State.

The Contractor may suspend or close the account of any customer who has not paid the annual or monthly fees when due.

The Contractor shall provide a monthly Account Receivable report to the State for outstanding monthly account payments due to the State from both State Agencies and private monthly account customers.

The Contractor shall use the below guidelines with regard to contacting any past due non-governmental monthly account customer. An account shall be deemed past due when payment has not been received by the time called for in the Account Agreement. The Contractor is not responsible for any uncollected amounts.

The Contractor shall take the following actions according to the designated numbers of days following the issuance date of any invoice:

1. 30 days- Check lockbox or system information for recent payments processed, put any appropriate accounts on watch list if payment is not received, and alert account holder of overdue status via a second billing notice.
2. 60 days - Check lockbox or system information for recent payments processed, suspend access to the portal for any appropriate accounts if payment is not received, make a courtesy call to the account holder's phone number of record to notify the monthly account holder of their suspended status and the necessary process to get the account holder's service reinstated.
   1. If the Contractor reaches the account holder's voice mail, the Contractor shall leave a message.
   2. If the Contractor is unable to leave a message, speak with the account holder or if the phone number of record is wrong, the Contractor shall continue to follow the process defined in the bullet below.
3. 90 days - Refer to the State for collection. Move account from suspended to closed. If contacted about resuming service, explain that account holder must:
   1. Bring account balance current,
   2. Remit new annual account fee, and make prepayment for ongoing services, if required by State.

Once the information has been referred to the State for collection, the Contractor has no further obligation for the processing or attempted collection of past due amounts. The Contractor makes no guarantee of payment or collection for any portal services rendered.

**1.17.6.1 Credit Balance Reports**

The following reports regarding customer account credit balances on the books for 90 days or longer shall be submitted to IOT by the 15th of each month:

1. List of all closed accounts having a credit balance of less than Five Dollars ($5.00). Upon instructions from IOT, the Contractor shall clear out such accounts by debit memo.
2. List of all closed accounts having a credit balance in excess of Five Dollars ($5.00). The Contractor shall pay the credit balance to the customer and bill IOT for that amount.
3. List of all active accounts having a credit balance of greater than $100 for the past quarter. The Contractor shall bill IOT for the credit balance and shall remit the credit balance to the customer upon payment by IOT.
4. The Contractor shall make the payments required above before the next monthly report is made.

**1.17.6.2 Transaction Fees**

Transaction fees are charged per service. All transaction fees are be collected and passed through directly to the State.

All per-transaction charges shall be in accordance with the then-current IN.gov account agreements and applicable service schedules, and shall be subject to applicable sales and use taxes, which taxes may be charged by the Contractor in addition to the agree-to per-transaction charges.

**1.18 Quality Assurance**

The Contractor must have a dedicated Quality Assurance (QA) team, including a dedicated Analyst. The Contractor is responsible for developing and establishing quality assurance standards and measures for the information technology services within the Contractor's organization for the IN.gov Web Portal. The Contractor shall also gather and analyze data in support of business cases, proposed projects, and systems requirements for the IN.gov Web Portal. This shall include writing test plans and scripts for testing during development and User testing and for tracking defects and fixes both during development and post deployment.

The Contractor shall apply proven analytical and problem-solving skills to help validate IT processes through careful testing in order to maximize the benefit of business investments in IT initiatives.

In addition to testing applications developed by the Contractor, the Contractor must maintain a test environment for testing all IN.gov-supported third-party Application updates and upgrades prior to release.

For the IN.gov portal and applications developed by the Contractor, the Contractor will:

1. Develop and establish quality assurance measures and testing standards for new applications, products, and/or enhancements to applications throughout their development/product lifecycles
2. Analyze documentation and technical specifications of any new application
3. Conduct internal audits to measure and assure adherence to established QA standards for software development, application integration and information system performance, and corresponding documentation
4. Create and execute test plans
5. Perform testing activities that demonstrate whether applications meet business requirements
6. Collaborate with software/systems personnel in application testing, such as system, unit, regression, load, and acceptance testing methods
7. Communicate test progress, test results
8. Test any new software with respect to functional requirements, system compliance, and technical specifications
9. Analyze formal test results with respect to defects, bugs; errors, configuration issues, and interoperability flaws
10. Assist in the development of change control processes, practices, and guidelines for new and existing technologies

**1.19 Initial Transition**

Prior to taking over the Scope of Work noted in this RFP, the Contractor shall work with the State to develop and manage an Initial Transition Plan for transferring services from the incumbent vendors. The Initial Transition Plan must include a comprehensive check-off list of all Contractor start-up activities and be approved by the State. The Contractor shall oversee the successful implementation of the Initial Transition Plan. The schedule and activities may be subject to adjustments made collaboratively by the Contractor and the State.

The Contractor shall complete the following tasks and activities during the Initial Transition period:

1. Develop an Initial Transition Plan, subject to State approval, including a detailed schedule and resources (quantity, type, and role) who will be available for all months of the Initial Transition.
   1. The Initial Transition Plan shall outline the following:
      1. An initial Resource Usage Guide that includes Contractor roles and responsibilities, including the roles and responsibilities of any subcontractors
      2. Contractor point(s) of contact
      3. A schedule with key milestones and deliverables
      4. A schedule and cadence for Initial Transition meetings and post Initial Transition operational meetings with the State
      5. State team roles and responsibilities
      6. Contractor methods, mechanisms, and procedures that will be utilized to complete the transition
      7. Issues and risks that need to be addressed during the transition period
      8. A detailed plan(s) to transfer any relevant project documentation from the incumbent vendor
      9. A detailed plan(s) to transfer any work-in-progress from the incumbent vendor
      10. A detailed plan(s) to transfer any relevant technology, systems, or assets (e.g., code, software, licenses) from the incumbent vendor
2. Evidence of participation in and completion of all training provided by the incumbent vendor and/or the State in operations and procedures
3. If desired by the State, shadow the incumbent vendor and/or State on all aspects of current workflows, releases, and assignments
4. Creation of transition meetings with the State to execute the Initial Transition Plan
5. Ensure complete turnover of all in-progress artifacts and solution components.
6. Confirm full administrative edit access to all environments for appropriate staff.
7. Complete all activities in the Initial Transition Plan.

The Contractor shall ensure that all website and application migration transition activities (i.e., transitioning existing assets to a new platform or system) are complete prior to any work commencing on new website creation or development for a State Entity User. If the Contractor intends on transitioning websites and applications to a new platform or system, their pricing in Attachment D - Cost Proposal shall account for the fact that website creation or development for a State Entity User cannot commence until the transition of existing assets is complete.

**1.20 End of Contract Turnover**

The services to be performed under this Contract are vital to the State and must be continued without interruption. Procedures must be in place to ensure a seamless transition and uninterrupted service throughout the transition to a project successor at contract end. The State seeks to ensure that program stakeholders experience no adverse impact from the transfer of scope to either the State or to the successor contractor(s) when the Contract is complete or terminated early.

The Contractor is responsible for planning and performing end of contract turnover and disengagement activities. Disengagement includes transition planning to ensure a seamless operational transition to the State or its designee in the event of required contract transition. The Contractor shall work with the State to assure that all end of contract turnover tasks are completed and that all responsibilities are transitioned in a timely and effective manner.

The Contractor shall complete the following tasks and activities during the End of Contract Turnover period:

* + 1. Develop an End of Contract Turnover Plan, subject to State approval, including a detailed schedule and resources (quantity, type, and role) who will be available for all months of the End of Contract Turnover period.
  1. The End of Contract Turnover Plan shall outline the following:
     1. Contractor roles and responsibilities
     2. State roles and responsibilities
     3. A schedule with key milestones and deliverables
     4. Method to transfer information to the State and/or a successor contractor(s)
     5. An inventory of detailed documentation about operations, applications, architecture, and infrastructure, as well as any supporting information related to the technical architecture and infrastructure.
     6. An inventory of all work-in-progress that need to be completed by the State and/or a successor contractor(s)
     7. Plans for coordination and transition of specific responsibilities from the incumbent to the future contractor.
     8. An inventory of all relevant project artifacts created, maintained, and updated throughout the Contract term
     9. An inventory of project documentation, work-in-progress, technology, systems, and assets necessary for a successive Contractor to perform the duties of the Scope of Work
     10. An inventory of third-party products, software, and vanity URLs for which the licenses need to be transferred
     11. Conduct training of State staff or successor contractor(s) staff, in the operations and procedures performed by Contractor staff.
     12. Perform shadowing and training activities for the State and successor contractor(s)
     13. Transfer the following information to the State or a successor contractor(s) on a medium acceptable to the State:
         1. All relevant project artifacts created, maintained, and updated throughout the Contract term
         2. Project documentation, work-in-progress, technology, systems, and assets necessary for a successive Contractor to perform the duties of the Scope of Work
         3. Other documentation including, but not limited to:
  2. User, provider, and operations manuals
  3. Training materials
  4. Documentation of any interfaces developed to support business activities between contractors
     1. Participate in reverse shadowing for the State and/or successor contractor(s) staff on all aspects of workflows, releases, and assignments as requested by the State
     2. Be available to provide support as requested by the State

By the end date of the Contract, the Contractor must turn over all State property to the State, and Contractor’s access to all State infrastructure and facilities shall be terminated.

The State has the right to initiate the disengagement process for any service under the Contractor Scope of Work with thirty (30) calendar day’s written notice. The notice of termination initiates these disengagement activities and responsibilities.

**1.20.1 Data Center Turnover and Continuity**

If this Contract expires or is terminated, and IN.gov is hosted by a third-party at the time of termination or expiration, the State may enter into a separate agreement for the continued use of the Data Center. Contractor's agreement with the Data Center shall contain a provision allowing the assignability of Contractor's agreement to the State in the event the Contractor is no longer providing portal services to the State. The agreement shall also include provisions for the cooperation and reasonable assistance to the State in transitioning the service to the State. The Contractor warrants and represents that it has reached agreement with any third-party responsible for hosting with respect to these obligations.