RESPONSE TO:

West Virginia Office of the Cabinet Secretary

One-Stop-Shop Permitting Portal

CRFP 0201 SEC2600000001 – TECHNICAL PROPOSAL

DATE: December 4, 2025

Prepared by:

IBM Consulting
Brian Cunningham
West Virgina Lead Client Partner
Brian.cunningham@ibm.com

IBM **Consulting**

"International Business Machines Corporation ("IBM") is submitting this Proposal, for services that will be led by IBM's Consulting division ("IBM Consulting")

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1818626 **Doc Description:** One-Stop-Shop Permitting Portal -State of WV **Proc Type:** Central Master Agreement			**Reason for Modification:** Addendum No. 4
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2025-12-01	2025-12-04 13:30	CRFP 0201 SEC2600000001	5

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : IBM Corporatoin

Address :

Street : 300 Summers St. Suite 600

City : Charleston

State : West Virgina **Country :** United States **Zip :**25301

Principal Contact : Brian Cunningham

Vendor Contact Phone: (304) 552-0032 **Extension:** N/A

FOR INFORMATION CONTACT THE BUYER
Tara Lyle
(304) 558-2544
tara.l.lyle@wv.gov

Vendor Signature X **FEIN#** 13-0871985 **DATE** 4 December 2025

All offers subject to all terms and conditions contained in this solicitation

November 21, 2025

Tara Lyle
Buyer Supervisor
Department of Administration
Purchasing Division
2019 Washington St E
Charleston, WV 25305

Dear Ms. Lyle,

Thank you for the opportunity to respond to the State of West Virginia's Request for Proposal for the development and implementation of a comprehensive one stop shop permitting solution. IBM shares the State's vision of streamlining processes, improving accessibility, and enhancing the experience of citizens, businesses, and agency staff across departments.

IBM is a **well-established systems integrator with decades of experience delivering large, complex public sector modernization programs**—projects that require deep domain expertise, disciplined program management, and unwavering commitment to security, transparency, and on time delivery. We have successfully led some of the nation's most significant **digital transformation initiatives**, helping governments modernize operations, improve constituent engagement, and achieve measurable efficiency gains.

As a **Salesforce implementation leader**, IBM brings unparalleled expertise in designing and deploying secure, scalable, and user-friendly solutions. Our approach leverages proven best practices in **Salesforce Public Sector Solutions**, ensuring seamless integration with existing systems while providing a flexible platform that can evolve with West Virginia's future needs.

IBM maintains longstanding relationships with the State of West Virginia, including managing the State's Medicaid data warehouse in partnership with the WV Department of Human Services (DoHS). In that role, it is coordinating with the DoHS and other vendors to help improve outcomes for some of the State's most vulnerable foster children and families, serving as the preferred partner for creating the DoHS artificial intelligence roadmap, and delivering advanced analytics and reporting. These partnerships demonstrate IBMs commitment to West Virginia while validating its capacity to bring the right tools and assets for the job.

Ultimately, IBM represents the **safe, reliable, and experienced** trusted partner capable of delivering a modern permitting solution that meets today's needs while preparing the State for tomorrow's growth. We look forward to the opportunity to collaborate with West Virginia to realize this vision and to demonstrate how IBM's experience, innovation, and stability make us the right partner for this important initiative.

Upon the State's award of this work to IBM the parties will negotiate and sign a Statement of Work ("SOW") which will describe the scope of the work, our respective responsibilities, Charges, and other terms. The mutually signed SOW will be the final description of IBM Services and will supersede IBM's RFP Bid Response in the Order of Precedence.

Sincerely,

Brian Cunningham
IBM Lead Client Partner
304-552-0032
Brian.Cunningham@ibm.com

Table of Contents

Executive Summary 1
Addressing Critical Statutory Requirements 1
Automated Refund Processing (§5A-13-4) 1
Fast-Track Expedited Processing (§5A-13-3(c)(6), §5A-13-6) 1
Mobile-Ready Field Operations 1
Proven Digital Solutions Driving Economic Growth 2
IBM and Salesforce: Powering West Virginia's Permitting Transformation 2
Implementation Timeline 2
Implementation Timeline to Meet January 1, 2027 Deadline 3
IBM Client Innovation Center (CIC) Support 4
Continuous Innovation and Future-Readiness 4
Contra **Error! Bookmark not defined.**
Addenda Acknowledgement 5
Designated Contact 10
Subcontractor List 12
One-Stop Shop Permitting Solution Overview 14
Four-Layer Technology Stack 16
Public Portal (Experience Cloud) 16
Core Dashboard (Salesforce Public Sector Solutions) 16
Integration Architecture 16
Security and Compliance Framework 16
Solution Components Delivering Comprehensive Capabilities 17
Centralized Application Management 17
Automated Routing and Approvals 18
Seamless System Integrations 18
Customizable User Experiences 18
End-to-End Communication and Collaboration 19
Real-Time Tracking and Transparency 19
Document and Records Management 19
Mobile Accessibility 20
Digital Wallet for Payments and Refunds 20
Scalability and Adaptability 20
Continuous Improvement and Future-Readiness 20
4.2.1 Goals and Objectives 22
Functional Requirements 22
Unified Portal for Public Users 22
Agency Dashboards and Internal Workflows 22
Document and Data Management 23
Payment, Refund, and Financial Processing 23
Analytics and Reporting 23
Notifications and Communications 24
Accessibility and Mobile Functionality 24
Training and Adoption 24
Performance, Security, and Reliability 24
Scalability and Future Growth 25
Core Tenets of IBM's Project Management Methodology 61
Tools Utilized in the Engagement 62

Payment Method Management 63
Transaction Processing & History 63
Automated Refund Processing 64
Digital License & Permit Storage 64
Mobile Accessibility 65
Accessibility & Compliance 65
Technical Implementation 65
User Experience Benefits 66
Scalability & Future Enhancement 66
4.2.2. Mandatory Project Requirements 67
Migration Approach 79
Data Portability 79
Migration Options 79
Real-Time Integration Technologies 81
Real-Time Use Cases 82
Three-Tier Support Structure 82
Service Level Agreements 83
Plan Delivery: Within 6 Months of Contract Award 83
Data Portability & Ownership 84
Knowledge Transfer 84
Transition Support (6 Months - No Additional Cost) 84
Financial Terms 85
System Continuity 85
Maintenance Activities 85
Updates & Enhancements 86
Maintenance Windows 86
Support Channels 86
Performance Monitoring 86
Knowledge Base & Self-Service 86
Continuous Improvement 87
4.3. Qualifications and Experience: 88
4.3.1. Qualification and Experience Information 88
Multi-Cloud Platform Experience 89
Cloud Architecture Capabilities 90
Disaster Recovery Best Practices 90
Government-Specific DR Experience 91
Encryption Expertise 92
Access Control Implementation 92
Audit Trail & Logging 93
Data Privacy & Compliance 94
Security Standards Training & Implementation 94
Vulnerability Management Experience 95
Incident Response Capabilities 96
4.3.2. Mandatory Qualification/Experience Requirements 99
Exceptions and Clarifications 101
Key Assumptions 104
Solution Scope Boundaries 105

Executive Summary

Governor Patrick Morrisey's vision for West Virginia, as articulated in House Bill 2002, centers on transforming the state's permitting ecosystem into a catalyst for robust economic growth. The Governor recognizes that by streamlining and modernizing the permitting process, West Virginia can attract new investments, spur job creation, and foster sustained prosperity across its communities. House Bill 2002 underscores the need to eliminate duplication, increase transparency, and reduce response times—each a critical step toward making the state more competitive for business and economic development.

IBM's One-Stop-Shop Permitting Platform, powered by Salesforce, is designed to realize this vision by consolidating permits and licenses from seven state departments into one unified dashboard. By providing an efficient, transparent digital system hosted on Salesforce Public Sector Solutions and FedRAMP High Government Cloud, the platform enables agencies to collaborate seamlessly, cut through bureaucratic red tape, and empower businesses to launch projects more rapidly. This holistic approach not only fulfills the statutory mandate for a January 1, 2027 go-live but also positions West Virginia as an attractive destination for economic innovation and opportunity. Given the complexity and inter-agency coordination required for this initiative, IBM's experience delivering large, complex enterprise transformations for government clients positions us exceptionally well to guide West Virginia through this modernization.

Addressing Critical Statutory Requirements

Automated Refund Processing (§5A-13-4)

The platform includes sophisticated deadline tracking and automated refund capabilities that enable accountability. When an agency misses a processing deadline, the system automatically triggers a full refund of all fees charged directly to that agency's budget. Every application is time-stamped upon receipt, assigned permit-specific deadlines from a regulatory database, and monitored through escalation alerts at 75%, 90%, and 100% of the timeline. This enables transparency for applicants and maintains pressure on agencies to meet their commitments while providing complete audit trails for legislative oversight.

Fast-Track Expedited Processing (§5A-13-3(c)(6), §5A-13-6)

West Virginia businesses can opt for expedited processing through a dynamic cost calculation engine that enables fast-track fees never exceed the actual cost to expedite. The platform manages separate priority queues, shortened deadlines (typically 50% of standard time), and capacity monitoring to prevent overload. Applicants can upgrade from standard to fast-track with one click, and fast-track applications receive the same refund protection if agencies miss expedited deadlines.

Mobile-Ready Field Operations

The platform delivers fully mobile capabilities for inspectors and field personnel through iOS and Android apps with offline functionality. Inspectors can capture photos, complete checklists, record notes via voice-to-text, and leverage GPS location stamping—all syncing automatically when connectivity is restored. This enables real-time data capture and faster processing without requiring constant internet access.

Proven Digital Solutions Driving Economic Growth

Successes from other state and local governments using Salesforce platforms for licensing and permitting underscore the transformative potential of this approach:

- **Arizona Registrar of Contractors (AZROC):** Saved 8,000 hours in annual data entry, reduced application deficiencies by 59%, customer inquiries by 18%, and cut costs by $125,000 per year.
- **State of Minnesota:** Simplified public access to nearly 600 types of licenses across five agencies, replacing paper forms and manual work with a centralized digital portal.
- **Wyoming Office of State Lands & Investments:** Improved data accuracy, consolidated legacy systems, enabled management of 40,000+ land parcels, and increased staff efficiency with a unified digital platform.
- **Massachusetts Department of Early Education and Care:** Streamlined license and inspection processes for over 11,000 providers using Salesforce, enabling online applications, real-time mobile inspections, and centralized communication, with 50 new applicants monthly benefiting from improved efficiency and automated workflows.
- **U.S. Department of Agriculture (USDA):** A $150B+ agency with 100,000 employees and 17 agencies has leveraged Salesforce to standardize and streamline its licensing, permitting, and collaboration processes across 12 integrated systems, resulting in consistent user experiences and improved data accessibility.

IBM and Salesforce: Powering West Virginia's Permitting Transformation

IBM stands out as the ideal team to implement West Virginia's one-stop-shop platform, underpinned by its status as a Salesforce Global Strategic Partner—one of Salesforce's top 30 partners worldwide. With more than 25 years of close collaboration with Salesforce and a proven track record of over 10,000 successful Salesforce implementations, IBM combines deep technical knowledge with unmatched global reach. Our team is made up of skilled professionals who hold more than 22,700 certifications—including Salesforce Public Sector Solutions—and operate out of eighteen global Technology Centers.

The proposed solution addresses West Virginia's specific challenges:

- **Redundant Processes:** A unified digital application portal consolidates all permit types, ensuring applicants submit information only once while agencies access centralized records.
- **Lack of Transparency:** Self-service dashboards, real-time status tracking, and proactive notifications build trust and clarity at every stage for applicants, businesses, and agency leaders.
- **Inefficient Coordination:** Cloud-based collaboration tools enable seamless communication between agencies, automatic handoffs, and centralized document management, breaking down silos.
- **Administrative Burden:** End-to-end workflow automation reduces manual steps, improves data accuracy, and shortens overall permitting timelines in full alignment with HB 2002's mandate to accelerate response times.

Implementation Timeline

With contract award anticipated in December 2025, IBM proposes a 13-month implementation schedule to meet the statutory January 1, 2027 deadline:

Implementation Timeline to Meet January 1, 2027 Deadline

Phase 1: Discovery & Foundation (Months 1-3)

- Help agencies complete July 2025 statutory reporting requirement
- Requirements workshops with all 7 departments
- Assessment of existing systems for integration
- Data migration planning
- Security baseline establishment
- Deliverable: Requirements document, system architecture

Phase 2: Platform Build (Months 4-7)

- Configure Salesforce Government Cloud tenant
- Build permit registry (all permit types)
- Develop workflow engine with deadline rules
- Create refund automation logic
- Implement role-based access control
- Integrate payment gateway and SSO
- Deliverable: Functional sandbox environment

Phase 3: Integration (Months 8-10)

- Connect MuleSoft to agency legacy systems
- Build public portal
- Build agency dashboards
- Develop mobile inspection module
- Create AI chatbot (Salesforce Einstein)
- Configure reporting/analytics
- Deliverable: Integrated test environment

Phase 4: Testing & Training (Months 10-12)

- User acceptance testing with agencies
- Security testing and FedRAMP validation
- Load/performance testing
- Train-the-trainer sessions
- Create help documentation
- Deliverable: Production-ready system

Phase 5: Go-Live (Month 13: January 2027)

- Production deployment
- Hypercare support (24/7 for first 30 days)
- Issue resolution
- Performance monitoring

Phase 6: Transition Period (Jan-June 2027)

- Optional use period (paper applications still accepted)
- User adoption campaigns
- Continuous improvement based on feedback

Mandatory Use Begins: July 1, 2027 (dashboard becomes exclusive method)

IBM Client Innovation Center (CIC) Support

To strengthen delivery capacity and meet West Virginia's One-Stop-Shop Permitting Program schedule, IBM will leverage its U.S.-based Client Innovation Centers (CICs). These centers provide specialized delivery teams skilled in Salesforce Public Sector Solutions, integration engineering, and data analytics. The CIC model combines local presence with national reach—offering scalable resources, consistent quality controls, and cost-effective operations.

IBM's CIC teams work in close coordination with state agencies and onsite IBM consultants, supporting development, testing, and ongoing operations throughout the 13-month implementation and beyond. West Virginia will benefit from:

- **Accelerated delivery** through dedicated squads operating in multiple time zones for continuous progress.
- **Local collaboration** with government-focused professionals experienced in public-sector compliance and FedRAMP environments.
- **Workforce continuity**—all project activities performed within the United States, in full alignment with state and federal data-security mandates.
- **Innovation access**—connection to IBM's nationwide network of CICs and Centers of Excellence for AI, data, and cloud integration.

By integrating CIC resources into the project, IBM provides West Virginia with a delivery framework that scales efficiently, maintains high quality, and supports sustained technical advancement throughout implementation and operation.

Continuous Innovation and Future-Readiness

Salesforce delivers three major platform updates annually, each automatically pushed to all customers with new features, security enhancements, and innovations tailored to public sector needs. This enables West Virginia's solution remains current with the latest compliance mandates, accessibility guidelines, and cybersecurity protections without disruptive upgrades or costly migrations. The platform's modular architecture and configuration-over-code approach enable rapid addition of new permit types, license categories, and agency partners as West Virginia's needs evolve.

By leveraging Salesforce's ongoing innovation and IBM's comprehensive implementation expertise, West Virginia gains not only a cutting-edge permitting solution at launch but also a platform that evolves with the demands of modern governance—delivering a secure, adaptable, and sustainable public service for years to come.

Upon the State's award of this work to IBM the parties will negotiate and sign a Statement of Work ("SOW") which will describe the scope of the work, our respective responsibilities, Charges, and other terms. The mutually signed SOW will be the final description of IBM Services and will supersede IBM's RFP Bid Response in the Order of Precedence.

Addenda Acknowledgement

IBM acknowledges receiving Addendum 1, 2, 3 and 4. Signed Addenda Acknowledgment forms are provided on the following pages.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SEC26*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

IBM Corporation
Company

Authorized Signature

4 December 2025
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SEC2600000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

IBM Corporation
Company

Authorized Signature

4 December 2025
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SEC2600000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

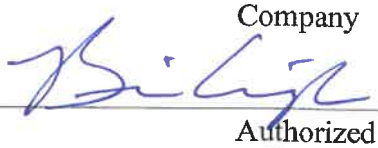
Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[X]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

IBM Corporation
Company



Authorized Signature

4 December 2025
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SEC2600000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[X]	Addendum No. 3	[ ]	Addendum No. 8
[X]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

IBM Corporation
Company


Authorized Signature

4 December 2025
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Designated Contact

IBM has provided a signed designated contact form on the following page.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Brian Cunningham, West Virigina Lead Client Partner

(Address) 300 Summers St, Suite 600; Charleston, WV 25301

(Phone Number) / (Fax Number) (304)552-0032 / NA

(email address) brian.cunningham@ibm.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes a binding offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

IBM Corporation
(Company)

(Signature of Authorized Representative)
Brian Cunningham, West Virigina Lead Client Partner
(Printed Name and Title of Authorized Representative) (Date)
(304)552-0032/ NA
(Phone Number) (Fax Number)
brian.cunningham@ibm.com
(Email Address)

Subcontractor List

IBM intends to self-perform this work. We have provided a complete subcontract list form on the following page.

Subcontractor List Submission (Information Technology)

Bidder's Name: IBM Corporation

☑ Check this box if no subcontractors will be provided access to State data, State information, or access to the State Network during the performance of this Contract.

Subcontractor Name	Work to be performed/Access to be granted	Additional Information for CIO Evaluation
Not Applicable.		

Attach additional pages if necessary

One-Stop Shop Permitting Solution Overview

House Bill 2002 identified several critical challenges within West Virginia's permitting process that directly impede economic development and frustrate businesses and citizens alike:

- **Redundant Processes:** Applicants face repetitive data entry, unclear requirements, and duplicative reviews across agencies, forcing them to navigate a maze of department-specific websites and submit identical information multiple times.
- **Lack of Transparency:** Applicants and stakeholders have limited visibility into permit status, requirements, and timelines, leading to frustration, delayed projects, and unnecessary status inquiries that burden agency staff.
- **Inefficient Coordination:** Agencies operate in silos with disparate systems, creating bottlenecks and making it difficult for leadership to track progress, identify issues, or resolve problems proactively.
- **Administrative Burden:** Manual workflows increase staff workload and the risk of human error, further delaying approvals and economic activity while diverting resources from higher-value tasks.

IBM's One-Stop-Shop solution, powered by Salesforce Public Sector Solutions on FedRAMP High Government Cloud, is expressly architected to overcome these pain points through a comprehensive four-layer technology stack.

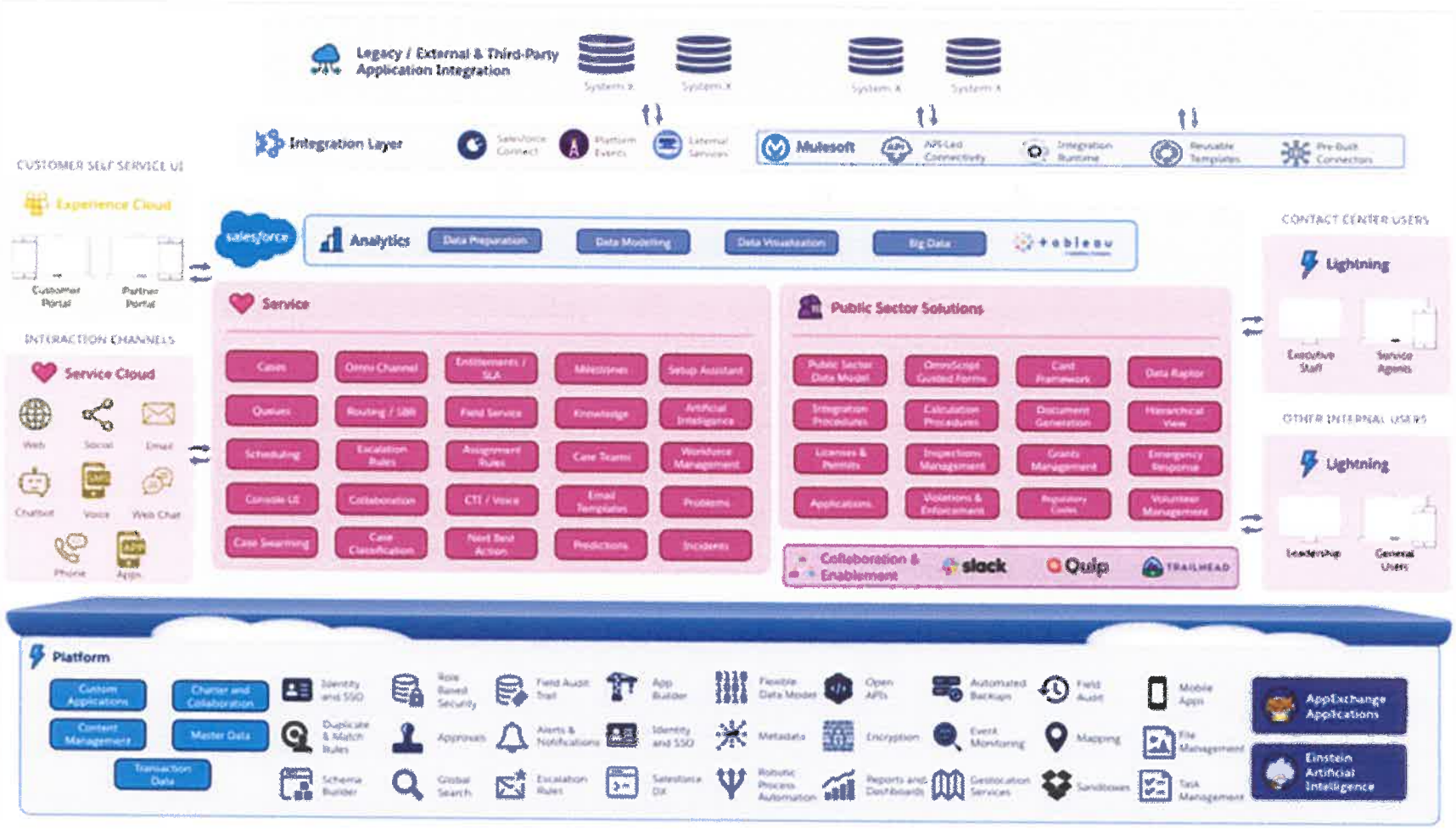


Figure 1 Salesforce Public Sector Solution Architecture

Four-Layer Technology Stack

Public Portal (Experience Cloud)

The citizen and business-facing portal provides an intuitive, accessible gateway to all permitting services. Users can log in once using Single Sign-On (SSO) integrated with the state's identity management system, then access any permit type across all seven participating departments from a single dashboard. The portal features online applications with intelligent, guided forms that adapt to permit type, secure document uploads from desktop or mobile devices, real-time status tracking with countdown timers, and integrated payment processing supporting credit cards, ACH, and digital wallet options. An AI chatbot – powered via Einstein provides 24/7 assistance, answering common questions and guiding users through complex processes. The entire portal is mobile-responsive and fully compliant with ADA and WCAG 2.2 AA accessibility standards.

Core Dashboard (Salesforce Public Sector Solutions)

At the heart of the system lies a master permit registry that consolidates all permit types across all participating agencies into a unified data model. The sophisticated workflow engine orchestrates application routing, review assignments, approval processes, and deadline tracking with escalation alerts at 75%, 90%, and 100% of statutory timelines. The automated refund processor monitors every application against its deadline, automatically triggering full fee refunds charged to the responsible agency's budget when deadlines are missed. Fast-track queue management provides separate priority processing pathways with shortened timelines for applicants who opt for expedited service. Inter-agency coordination tools enable seamless handoffs, shared case notes, and collaborative reviews for permits requiring multiple departmental approvals.

Integration Architecture

The platform leverages Salesforce's robust native integration capabilities as the primary approach, utilizing Salesforce Connect for real-time external data access, REST and SOAP APIs for system-to-system communication, Platform Events for event-driven workflows, Bulk API for large data transfers, and scheduled batch processing for legacy system synchronization. For more complex scenarios involving numerous legacy systems (10+), high transaction volumes (1M+ annually), or extensive data transformation requirements, the solution can incorporate MuleSoft Anypoint Platform as an enterprise integration layer. This flexible approach enables bidirectional data synchronization with existing permit tracking systems across all seven departments while maintaining connections to payment gateways, the state's identity management system, financial and ERP systems, address verification services, email and SMS notification platforms, document storage, GIS systems for location-based permits, and electronic signature services.

Security and Compliance Framework

The solution implements a multi-layered security architecture designed to protect sensitive licensing and permitting data at every level. Granular role-based access control (RBAC) enables that public applicants, agency staff, administrators, and auditors access only the information necessary for their roles, enforced through least privilege principles. Single Sign-On (SSO) integration with Multi-Factor Authentication (MFA) provides centralized authentication while maintaining strict access controls. All data is encrypted both in transit using TLS 1.3 and at rest using FIPS 140-3 compliant Advanced Encryption Standard (AES-256). Salesforce Shield Platform Encryption protects PII, Social Security numbers, payment data, and proprietary business information with field-level encryption and comprehensive audit trails. The platform

maintains FedRAMP High authorization and implements NIST SP 800-53 Rev 5 controls, with 24/7 security monitoring, automated vulnerability scanning, annual penetration testing, and complete audit logging with 7-year retention per state records policy.

Solution Components Delivering Comprehensive Capabilities

Centralized Application Management

The unified digital platform transforms the permitting journey by consolidating disparate processes into a single portal that adapts to each applicant's unique needs. Whether applying for a simple license renewal or managing a complex multi-agency project, applicants engage with streamlined workflows that provide real-time guidance, centralized document storage, and the ability to manage multiple permit types concurrently. For agency personnel, the centralized workspace offers role-based access with applications automatically organized, categorized, and prioritized, eliminating manual tracking and reducing oversight risks. Integrated analytics and reporting tools monitor performance, identify bottlenecks, and enable compliance with HB 2002 requirements. Every touchpoint is logged and auditable, with applicants receiving automated updates that significantly reduce status inquiries and enable staff to focus on higher-value activities.

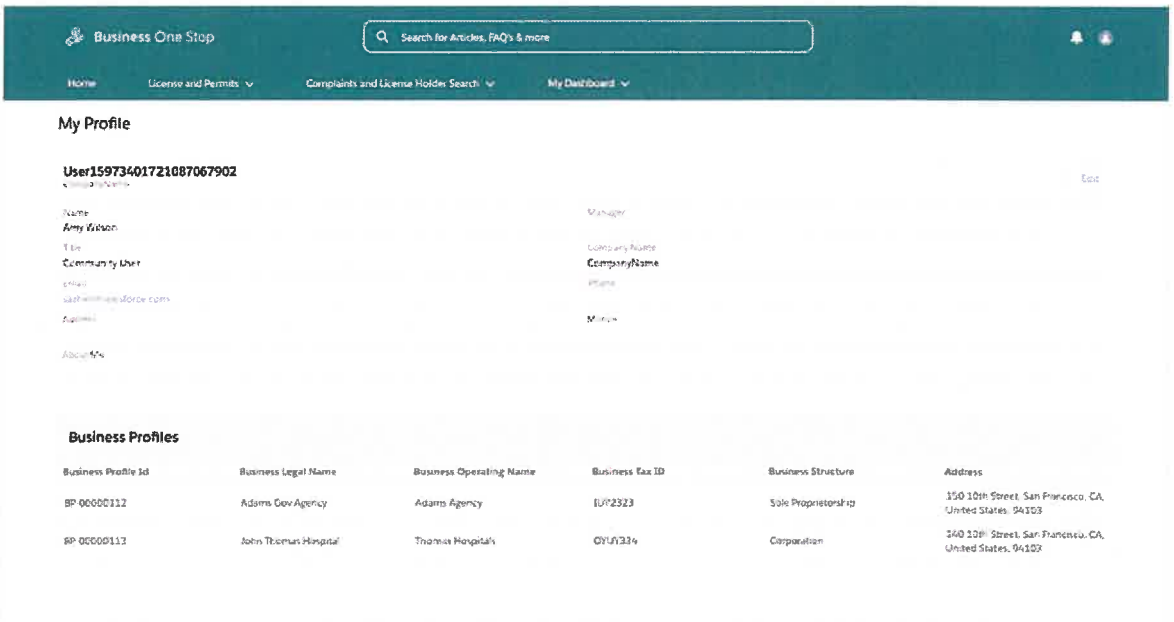


Figure 2 Registered users have access to everything they need in regard to licensing, permits, and inspections

Automated Routing and Approvals

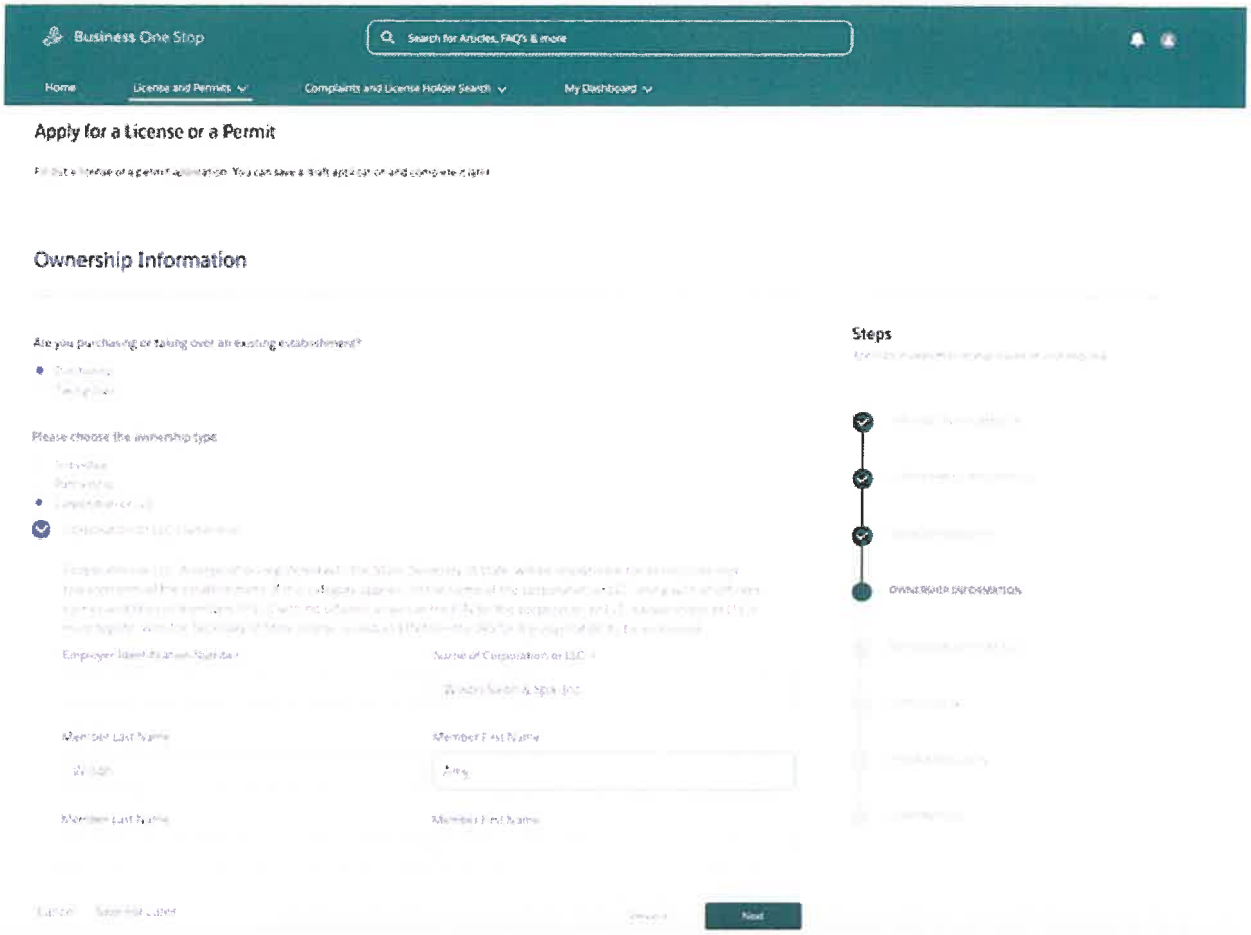
Advanced workflow automation orchestrates every step with precision, intelligently routing applications based on permit type, project complexity, jurisdictional boundaries, and required departmental reviews without manual intervention. The robust rules engine codifies business logic and compliance requirements directly into workflows, automatically triggering escalations for high-risk applications or routing files for additional environmental or legal scrutiny. When supporting documentation is incomplete, automated notifications request clarification, reducing delays. Straightforward applications may receive instant approval after automatic checks, while complex cases follow multi-stage review processes with sequential or parallel input from different departments. Built-in analytics monitor workflow efficiency, flagging bottlenecks and enabling proactive intervention through service-level agreements that automatically escalate stalled applications to supervisors.

Seamless System Integrations

MuleSoft and Salesforce's native APIs enable effortless integration with existing state systems including GIS, tax, inspection, and payment solutions, ensuring real-time data exchange and eliminating manual data entry burdens. Agencies can automatically validate applicant information against authoritative state databases, verify parcel data through GIS mapping, synchronize permit fees with financial systems for accurate invoicing, and share inspection schedules and compliance records between departments. The system's open architecture allows easy expansion as new technologies or regulatory requirements emerge, supporting connection of future data sources or partner agencies while providing a holistic view of permit activity across the state.

Customizable User Experiences

Role-based portals and dashboards deliver tailored access and functionality for every stakeholder. Applicants benefit from intuitive step-by-step application wizards with draft-saving features (auto-saving every 30 seconds), automated status notifications, and secure document uploads from desktop or mobile cameras. Agency staff across West Virginia's diverse departments receive personalized queues and dynamic task lists that prioritize urgent items and manage caseloads efficiently. Real-time analytics dashboards present actionable insights on permit volume trends, recurring compliance issues, and service-level performance. Integration with state-specific systems means personnel no longer grapple with siloed data or redundant entry—information flows seamlessly between the platform and existing West Virginia databases for parcel records, applicant credentials, and compliance documents.



End-to-End Communication and Collaboration

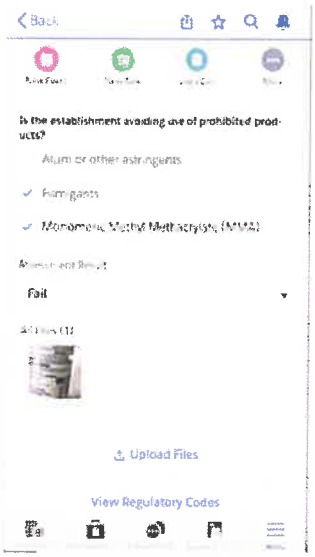
In-platform messaging, automated reminders, and inter-agency workgroups break down communication barriers. Stakeholders can submit and track inquiries, attach supporting documents, and collaborate on compliance reviews all within the secure Salesforce environment. Email and SMS notifications keep all parties informed at critical milestones, while shared case notes and escalation workflows facilitate resolution of complex applications requiring multiple departmental inputs.

Real-Time Tracking and Transparency

Applicants and agency leadership access real-time dashboards providing transparent views into the entire permitting process, highlighting application status, outstanding tasks, workflow bottlenecks, and compliance with HB 2002 benchmarks. Comprehensive audit trails automatically log every action—whether a permit approval, document upload, or inter-departmental communications supporting smooth internal audits and enabling complete reconstruction of any permit's history for regulatory compliance. Public reporting features allow non-sensitive permit data, processing times, and compliance outcomes to be published on citizen-facing portals, enabling residents, businesses, and watchdog organizations to independently monitor agency performance and hold public institutions accountable.

Document and Records Management

All documents, plans, correspondence, and approvals are centrally stored with version control and easy retrieval, ensuring compliance with public records laws and facilitating smooth audits. The system maintains complete chain-of-custody documentation with tamper-evident audit trails and supports both active case management and long-term archival requirements.



Mobile Accessibility

The platform is fully mobile-ready, leveraging Salesforce's advanced mobile capabilities through native iOS and Android apps. Field inspectors, agency staff, and applicants can securely access the system from smartphones or tablets with intuitive interfaces that support capturing and uploading site photos, annotating documents, completing digital checklists, and submitting inspection reports directly from the field. Push notifications alert users to critical updates and deadlines, while GPS integration enables geo-tagging of inspection locations. Offline access allows work to continue in areas with limited connectivity, automatically syncing data once connection is restored.

Digital Wallet for Payments and Refunds

The integrated digital wallet capability streamlines financial transactions throughout the permitting lifecycle. Citizens and businesses can store multiple payment methods (credit cards, debit cards, bank accounts) for one-click payment on applications and automatic payment for renewals (opt-in). The PCI-DSS compliant payment gateway supports all major credit cards, ACH/eCheck capability, and payment plans for high-value permits with installment options. When refunds are triggered by missed deadlines, the system automatically returns funds to the original payment method or provides alternative refund methods if the original has expired. The wallet also stores digital copies of all active permits and licenses with QR codes for verification by inspectors, expiration date reminders, renewal links, and downloadable PDFs.

Scalability and Adaptability

The solution's modular, cloud-first architecture enables West Virginia can rapidly adapt to evolving needs. Most business logic and workflows are delivered via Salesforce's declarative tools—Flow, Process Builder, and custom objects—enabling agencies to rapidly design, deploy, and update processes with minimal custom development. When new permit types, license categories, or regulatory requirements emerge, staff can configure new forms, approval workflows, data validation rules, and notification triggers directly within the platform's intuitive interface, often entirely by agency administrators or business analysts. Additional agencies and their unique permitting requirements can be onboarded seamlessly through standardized templates and reusable components, while agency-specific needs are easily accommodated through configuration. Salesforce's AppExchange ecosystem enables agencies to add specialized modules or vetted third-party solutions without compromising security or interoperability.

Continuous Improvement and Future-Readiness

Salesforce operates on a robust release cycle, delivering three major platform updates annually with new features, security enhancements, and innovations automatically pushed to all customers—ensuring West Virginia's solution remains current without disruptive upgrades or costly migrations. The platform's proactive approach to security incorporates the latest advances in cyber defense, encryption, access control, and threat detection with every update, informed by collaboration with government security experts and real-world intelligence. Regular penetration testing, compliance audits, and transparent trust reporting provide ongoing assurance to government staff and the public. This future-ready foundation empowers agencies to quickly respond to legislative changes, public expectations, and technological advancements while maintaining a secure, adaptable, and sustainable public service.

4.2.1 Goals and Objectives

Functional Requirements

IBM's proposed One-Stop-Shop Permitting Portal fulfills every functional requirement outlined in the RFP and delivers all capabilities requested by the State of West Virginia. Built on Salesforce Public Sector Solutions and hosted within Salesforce Government Cloud Plus, the platform provides a comprehensive suite for permitting and licensing that unifies application submission, tracking, inspection, payment, refund, and reporting in a single secure system.

The solution replaces scattered permit systems with a single digital environment accessible through role-specific dashboards for citizens, businesses, and agency staff. It offers workflow automation, document and payment handling, integrated data management, and transparent reporting that promote accountability and efficiency.

IBM's implementation meets accessibility standards, supports mobile operations, and integrates with existing state infrastructure while maintaining full FedRAMP High compliance. The architecture is designed for future expansion without replacement, allowing new agencies and permit types to be added through configuration. Training and support plans build internal capability for long-term success, giving the State a modern permitting platform that is transparent, efficient, and ready to sustain economic growth well beyond initial deployment.

Unified Portal for Public Users

The public portal gives applicants a single point of access to all participating departments. It presents guided forms that adapt to the type of permit selected. Once an application is created, the user receives a clear view of progress from submission to approval. The interface displays stages such as "Submitted," "Under Review," "Inspection," "Approved," and "Issued." Each stage contains time tracking so applicants can see how long each step takes.

The portal supports document uploads, digital signatures, and online payments. It also provides a digital wallet that stores active permits and receipts. Citizens can log in to renew licenses, request modifications, or apply for additional permits without repeating basic information. The design follows accessibility standards under WCAG 2.2 AA and Section 508 so all residents can interact with the system regardless of ability or device type. Mobile access is fully supported through responsive web pages and Salesforce mobile applications.

Notifications keep users informed throughout the process. Email or SMS alerts announce key events such as submission confirmation, requests for additional documents, inspection scheduling, or approval. Users can choose how they receive these alerts. They can also view a complete timeline of actions in their dashboard which adds transparency and reduces calls to agency offices.

Agency Dashboards and Internal Workflows

Agency personnel will operate through role-based dashboards built with Salesforce Public Sector Solutions. Each department will have a workspace tailored to its responsibilities. Reviewers can view assigned applications, check completeness, add comments, and make decisions with one click. Supervisors will have access to workload views that display pending tasks and performance indicators. Executives will see reports that summarize processing times, approval rates, and refund activity.

Workflows will be automated across all departments. When a citizen submits an application, the system routes it to the correct agency based on permit type and geographic location. If multiple

departments must participate, the system creates parallel review paths so work can progress without delay. Built-in business rules trigger escalations when deadlines approach or when applications require higher-level approval. These rules are configurable through Salesforce Flow so agency staff can adapt them without programming.

The inspection module gives field officers a mobile tool for on-site work. Inspectors will record findings, capture photos, and add notes even when offline. Data syncs automatically once connectivity returns. This eliminates paper forms and manual entry after returning to the office. Inspection results appear instantly in both the applicant's dashboard and the agency's internal view.

Document and Data Management

Document handling is a core capability of the platform. Applicants and staff can upload files such as site plans, insurance certificates, or environmental assessments. All files are stored in Salesforce Files with version control. Authorized users can view, annotate, and mark documents as accepted or rejected. Audit trails record every action on each file including who accessed it and when.

Data integrity is maintained through structured migration and validation activities. Legacy records from existing systems will be cleansed and imported into Salesforce Government Cloud. During migration IBM will map fields, remove duplicates, and verify completeness. Approximately two terabytes of data and several hundred thousand paper files will be digitized. After migration, all permit data will reside in one master registry accessible to authorized agency staff.

Real-time data exchange connects the portal to external systems. Salesforce native APIs will provide initial integration with payment gateways, GIS mapping, and state financial applications. If deeper integration becomes necessary across multiple agencies, MuleSoft Anypoint Platform will be introduced to extend connectivity. This phased approach allows immediate functionality while leaving room for future expansion.

Payment, Refund, and Financial Processing

The system includes full payment capability through PCI-DSS-compliant gateways. Applicants can pay fees using credit cards, ACH, or digital wallets such as Apple Pay or Google Pay. Receipts are generated automatically and stored in the user's account. Agency financial systems receive transaction data through secure APIs for reconciliation.

Automated refund logic fulfills the statutory requirement for deadline accountability. When an agency exceeds its processing time, the portal triggers a refund directly to the applicant's original payment method. The workflow calculates fees, records the reason for refund, and updates agency budget reports. This function supports state transparency goals and reduces manual accounting effort.

Analytics and Reporting

Salesforce CRM Analytics and Tableau will provide dashboards for both operational and executive users. Agencies can view metrics such as number of applications received, average processing time, inspection volume, and refund totals. Dashboards will refresh in real time and support drill-down analysis. Reports can be exported to Excel or PDF for internal review or publication on public websites. These analytics help leadership identify bottlenecks, allocate staff, and track compliance with performance targets set by House Bill 2002.

Public transparency is a major part of the functional design. Non-confidential data may be displayed on a public dashboard showing statewide permit activity and agency turnaround

times. This builds confidence in government operations and provides measurable evidence of improvement.

Notifications and Communications

Communication features go beyond basic email. The portal includes in-platform messaging that allows applicants and reviewers to exchange notes without external email threads. Each message is stored with the application record creating a full history of correspondence. Automated reminders prompt both applicants and staff when actions are pending. These features reduce missed deadlines and improve collaboration between agencies.

Users can personalize their communication settings. They may prefer daily summaries or immediate alerts depending on their workflow. The system records preferences and applies them automatically. All notifications follow accessibility rules and are available in multiple languages where required.

Accessibility and Mobile Functionality

Accessibility and mobility are fundamental design elements. All screens use clear layouts, high-contrast colors, and readable text sizes. Keyboard navigation and screen-reader compatibility are built into Salesforce Experience Cloud. Mobile performance is optimized through responsive components that load quickly on cellular networks. Inspectors in remote areas can complete work offline and synchronize later. Citizens can apply for permits, upload documents, and make payments from any smartphone or tablet.

Training and Adoption

IBM's train-the-trainer model prepares agency champions to support colleagues after deployment. Each agency will select two or three staff members who will participate in intensive workshops covering system navigation, workflow management, and troubleshooting. IBM will provide digital learning materials through Salesforce Trailhead and the portal's help center. These materials include step-by-step guides, short videos, and self-tests. The approach allows continuous learning as new features become available.

Change management activities will promote adoption across agencies. Communications will highlight success stories and improvements in turnaround time. Feedback collected through surveys and focus groups will guide further refinements during maintenance cycles.

Performance, Security, and Reliability

Performance testing will confirm that the system can handle expected volumes of 50,000 applications per year and concurrent access by hundreds of users. Load tests will simulate peak conditions to verify response times. The environment operates in Salesforce Government Cloud Plus which meets FedRAMP High standards. All data is encrypted at rest with AES-256 and in transit with TLS 1.3. Multi-factor authentication protects user accounts. Audit logs capture every action for seven years supporting legal and regulatory review.

IBM's support model includes Level 2 and Level 3 coverage during business hours with on-call response for critical incidents. Customer support and contact-center services can also be provided by IBM if requested. Detailed staffing and service levels will be confirmed during the Discovery Phase when call volumes and user needs are better understood. The combination of proactive monitoring and structured support keeps operations stable throughout the contract term.

Scalability and Future Growth

The solution is built to expand as new agencies join. Adding a department requires only configuration of new permit types and user roles. No code changes are needed. The architecture supports unlimited external users and up to 500 internal staff seats at launch. Additional capacity can be added through license adjustments. Salesforce delivers three major platform updates each year which introduce new features automatically. IBM will review each release and apply relevant improvements during quarterly maintenance windows.

4.2.1.1 Vendors should provide a methodology and explain in detail how they would develop and create a user-friendly dashboard interface with public-facing, and internal agency components as a One-Stop-Shop Permitting Portal.

IBM employs a structured, human-centered methodology to develop the One-Stop-Shop Permitting Portal. The approach combines Enterprise Design Thinking-driven discovery, Salesforce Public Sector Solutions (PSS) configuration on FedRAMP High Government Cloud using declarative development, interactive CRM Analytics dashboards, integration with existing agency systems, and continuous improvement through training and maintenance.

Discovery and Design:

IBM begins with collaborative discovery establishing user needs and technical requirements:

- **Stakeholder workshops:** Document workflows, permit types, pain points across all seven agencies
- **User research:** Interview citizens, businesses, reviewers, inspectors, and leadership
- **Persona development:** Create profiles representing key user types
- **Journey mapping:** Document current-state processes and design future-state experiences
- **Accessibility planning:** WCAG 2.2 AA and Section 508 compliance from inception
- **Rapid prototyping:** Wireframes and mockups validated through user playback sessions
- **Solution blueprint:** Define portal structure, dashboards, integrations, security architecture
- **Design system:** Establish State branding and UI components

Public-Facing Dashboard (Experience Cloud):

The public portal provides personalized, self-service access for citizens and businesses:

- **Personalized home page:** Active applications, renewals, notifications, quick actions
- **Status tracker:** Visual progress indicators with elapsed time and estimated completion
- **Portfolio view:** All permits/licenses with filtering and sorting
- **Document center:** Upload files, view status, download approved permits
- **Payment dashboard:** Transaction history, fees, stored payment methods, receipts
- **Self-service actions:** Apply, renew, pay, upload, contact agency
- **Mobile-responsive:** Seamless adaptation to smartphones and tablets
- **Accessibility:** Screen reader compatible, keyboard navigation, bilingual (English/Spanish)

Internal Agency Dashboards (Public Sector Solutions):

Agency staff receive role-based workspaces optimized for their functions:

- **Reviewer workspace:** Queue-based dashboard with urgency sorting and deadline indicators
- **360-degree view:** Complete applicant history, related permits, communications, payments
- **Workflow tools:** One-click approve/deny, document annotation, collaboration
- **Performance metrics:** Applications processed, review times, pending workload
- **Supervisor dashboards:** Team performance, workload distribution, SLA compliance

- **Executive dashboards:** Enterprise-wide volume, revenue, efficiency, refund costs
- **Inspection management:** Mobile-enabled with offline capability
- **Compliance monitoring:** Deadline countdowns, at-risk applications, refund exposure

Integrated BI Dashboards & Reports (if required for advanced analytics):

Interactive dashboards provide real-time insights and visualization:

- **Pre-built templates:** Salesforce PSS templates customized for West Virginia
- **Low-code builder:** State administrators create/modify dashboards without programming
- **Interactive visualizations:** Charts, graphs, heat maps with drill-down capability
- **Real-time refresh:** Automatic updates as applications progress
- **Embedded analytics:** Contextual insights at point of decision
- **Predictive analytics:** CRM Analytics forecasting and risk identification
- **Scheduled reports:** Automated generation and distribution
- **Self-service reporting:** Ad-hoc report creation by staff

Integration Architecture:

Flexible integration strategy connects existing systems and services:

- **Assessment-driven:** Discovery determines optimal approach (Salesforce-native vs. MuleSoft)
- **Agency systems:** Real-time or batch integration with existing permit tracking
- **Payment gateway:** PCI-DSS compliant with automated refund capability
- **SSO integration:** SAML 2.0/OpenID Connect with State identity management
- **Financial systems:** State accounting/ERP integration for revenue tracking
- **Supporting services:** Address verification, notifications, document storage, GIS, e-signature
- **API-first design:** RESTful APIs for future extensibility
- **Error handling:** Automated retry, logging, reconciliation

Security and Quality:

Enterprise-grade security and compliance controls:

- **FIPS 140-3 encryption:** AES-256 at rest, TLS 1.3 in transit
- **FedRAMP High:** Government Cloud with continuous monitoring
- **Multi-factor authentication:** Required for all users
- **Role-based access:** Granular permissions by user role
- **WCAG 2.2 AA compliance:** Full accessibility testing
- **Performance testing:** Load testing at 3x expected volume
- **Security testing:** Vulnerability scanning, penetration testing
- **User acceptance testing:** Validation by representative users

Training and Governance:

Comprehensive change management enables successful adoption:

- **Train-the-trainer:** 2-3 champions per agency train colleagues
- **Role-based training:** Targeted curricula by user type
- **Hands-on labs:** Practice in sandbox environment
- **Knowledge base:** Articles, videos, FAQs, troubleshooting guides
- **Change management:** Communication plans, sponsorship, adoption campaigns

Continuous Improvement:

Structured maintenance enables long-term platform sustainability:

- **Monthly:** Health checks, performance tuning, security patches, minor enhancements
- **Quarterly:** Feature releases, usability testing, disaster recovery drills, business reviews
- **Annual:** Platform upgrades, roadmap planning, security audits, satisfaction surveys
- **Hybrid Agile enhancements:** Prioritized backlog with 4-6 week delivery cycles
- **User feedback:** Surveys, focus groups, analytics informing refinements
- **Configuration flexibility:** Low-code tools enabling State self-sufficiency

This methodology delivers intuitive, accessible dashboards simplifying permit processes for citizens while providing agency staff powerful tools for efficient review, collaboration, and performance management—all within a secure, compliant platform adapting to West Virginia's evolving needs.

4.2.1.2 Vendors should describe how they would implement a flexible and secure Role Based Access Control system.

IBM implements Role-Based Access Control (RBAC) leveraging Salesforce Public Sector Solutions' native security capabilities combined with Zero-Trust principles, NIST SP 800-53 controls, and OWASP best practices. The RBAC framework provides granular control over data, workflows, and functionality while maintaining scalability, auditability, and compliance with federal and state security standards.

Design Principles:

IBM's RBAC approach follows four foundational security principles:

- **Least privilege:** Users granted only permissions necessary for assigned duties
- **Separation of duties:** Sensitive functions divided across roles reducing fraud/error risk
- **Granular inheritance:** Access managed at organization, object, field, and record levels with inheritance simplifying administration
- **Scalability and flexibility:** Model adapts easily to organizational changes, new programs, and regulatory requirements without reengineering

Discovery and Security Architecture:

During discovery, IBM security architects collaborate with State leadership, cybersecurity staff, and program managers to define the access control model:

- **Role identification:** Document all user types (application reviewers, inspectors, supervisors, executives, public applicants, business users)
- **Permission mapping:** Define required access for each role (view, create, edit, delete, approve) by data type and workflow stage
- **Sensitivity classification:** Identify PII, financial data, enforcement actions, and other sensitive information requiring restricted access
- **Compliance requirements:** Enable model meets NIST 800-53, FedRAMP, and State cybersecurity policy mandates
- **Organizational structure:** Map State agency hierarchy, departmental boundaries, and inter-agency collaboration needs
- **Workflow analysis:** Understand handoffs, escalations, and collaboration patterns requiring shared access

Multi-Layered Security Configuration:

IBM implements Salesforce's native multi-layered security model providing defense-in-depth:

- **Organization-Level Access:**
  - Multi-Factor Authentication (MFA) required for all users
  - IP address restrictions for administrative accounts
  - Session timeouts (15 min public, 30 min staff)
  - Login hours enforcement (optional by role)
  - Device activation policies
- **Profile-Level Access:**
  - Baseline profiles for each functional area (Licensing Agent, Field Inspector, Supervisor, Administrator, Public Applicant)
  - Object permissions defining CRUD rights (Create, Read, Update, Delete)
  - Tab visibility controlling which application areas accessible
  - App permissions determining which Salesforce apps users can access
  - Administrative permissions (e.g., "View All Data," "Modify All Data") restricted to authorized administrators only
- **Permission Sets and Groups:**
  - Modular privileges layered onto profiles for specialized access
  - Temporary permissions granted without modifying core profiles
  - Permission Set Groups bundling related permissions (e.g., "Fast-Track Reviewer" includes expedited queue access and financial approval)
  - Hybrid Agile adjustments as roles evolve without profile redesign
  - Easier auditing through discrete permission components
- **Object and Field-Level Security:**
  - CRUD controls on objects (Permit, Application, Inspection, Payment)
  - Field-level security hiding/protecting sensitive data (SSN, payment information, enforcement notes)
  - Read-only access for historical records preventing modification
  - Privacy compliance through PII field restriction
  - Encryption of sensitive fields using Shield Platform Encryption
- **Record-Level Security (Sharing Rules):**
  - Role hierarchy defining organizational structure and access inheritance
  - Public groups for cross-functional teams requiring shared access
  - Sharing rules granting access based on criteria (e.g., all permits in user's county)
  - Manual sharing for ad-hoc collaboration on specific records
  - Territory management for geographic-based access (optional)
  - Data isolation between agencies while enabling inter-agency coordination for multi-department permits
- **Authentication Controls:**
  - SSO via SAML 2.0/OpenID Connect integrated with State identity provider
  - MFA enforcement configurable by role and risk level
  - Password policies (complexity, expiration, reuse prevention)
  - Account lockout after failed login attempts
  - Trusted IP ranges for sensitive operations

Identity and Access Management (IAM) Integration:

IBM integrates Salesforce RBAC with the State's existing IAM infrastructure ensuring centralized identity governance:

- **Single Sign-On (SSO):** SAML 2.0 or OpenID Connect authentication through State identity provider eliminating separate credentials
- **Multi-Factor Authentication:** Required for all privileged roles; configurable for public users based on risk assessment
- **Just-in-Time (JIT) Provisioning:** Automatically creates/updates Salesforce accounts based on IAM attributes (department, position, clearance level)
- **Automated de-provisioning:** When IAM account disabled, Salesforce access immediately revoked through federation
- **Attribute-based access:** User permissions dynamically assigned based on IAM attributes (job title, department, certifications)
- **Centralized governance:** All access requests, approvals, and reviews managed through State IAM workflows

Zero-Trust Architecture:

Following Zero-Trust principles, IBM implements continuous verification:

- **No implicit trust:** Access not granted based on network location or device
- **Continuous authentication:** Session validity continuously verified throughout user interaction
- **Context-aware access:** Permissions adjusted based on device, location, time, and risk score
- **Micro segmentation:** Data and functionality segregated with explicit access grants required
- **Audit and analytics:** All access attempts logged and analyzed for anomalies

Role Examples and Permissions:

- **Public Applicant:**
  - View/edit own applications only
  - Upload documents, pay fees, view status
  - No access to other applicants' data or agency back-office
- **Application Reviewer:**
  - View/edit assigned applications within their agency/program
  - Approve/deny within authority limits
  - No access to other agencies' applications or administrative functions
- **Field Inspector:**
  - View assigned inspections
  - Create/edit inspection records
  - Mobile app access with offline capability
  - No access to financial data or approvals
- Supervisor:
  - View all applications within their department
  - Reassign work, override decisions, view team performance
  - No access to other departments without explicit sharing

- **Agency Administrator:**
  - Full access to their agency's data and users
  - Configure workflows, forms, reports for their agency
  - No access to other agencies' data or system-wide settings
- **System Administrator:**
  - Full system access for configuration and maintenance
  - User provisioning and role management
  - Security monitoring and audit review
  - Restricted to authorized IT personnel only

Ongoing Management and Governance:

IBM establishes processes ensuring RBAC remains effective and compliant:

- **Quarterly access reviews:** Automated reporting of user permissions with supervisor certification
- **Role lifecycle management:** Process for requesting, approving, provisioning, and deprovisioning access
- **Segregation of duties enforcement:** Automated detection of conflicting permission combinations
- **Audit logging:** Comprehensive logs of all access grants, modifications, and login attempts retained 7 years
- **Privileged access monitoring:** Enhanced logging and alerting for administrative actions
- **Training and awareness:** Role-based security training ensuring users understand their responsibilities
- **Change control:** All permission changes reviewed and approved through governance board

Flexibility and Scalability:

The RBAC system adapts to evolving State needs:

- **New agency onboarding:** Template roles replicated and customized for additional agencies joining platform
- **New permit types:** Permissions extended to cover new workflows without redesigning entire model
- **Organizational changes:** Role hierarchy and sharing rules updated to reflect agency restructuring
- **Emergency access:** Break-glass procedures for urgent situations with full audit trail
- **Self-service administration:** Delegated administrators can manage users and permissions within their scope using low-code tools

IBM's flexible, secure RBAC implementation protects sensitive data through granular access controls, enables compliance with federal and state security standards, adapts easily to organizational changes and new requirements, provides complete audit trails for accountability, and integrates seamlessly with State IAM infrastructure—delivering enterprise-grade security without sacrificing usability or operational efficiency

4.2.1.3 Vendors should explain how they will design a user-friendly, and responsive interface that tracks applications through the approval process and the ability to apply for additional permits or other licenses as needed.

IBM's solution features a responsive interface enabling constituents to track applications and apply for additional permits using saved information. Built on Salesforce Lightning Web Components, the interface automatically adapts to desktop, tablet, and mobile devices while maintaining accessibility and usability standards.

Human-Centered Design:

IBM's Enterprise Design Thinking approach enables intuitive, accessible design:

- **Stakeholder workshops:** Document needs with agency staff and users (business owners, contractors, inspectors)
- **Personas and journey maps:** Model user interactions identifying pain points
- **Rapid prototyping:** Validate mockups before development
- **WCAG 2.2 AA compliance:** Inclusive design for all users
- **Iterative refinement:** Continuous feedback incorporation

Responsive Foundation:

The platform provides consistent experiences across all devices:

- **Lightning Web Components:** Auto-adjust layouts for any screen size
- **Experience Cloud portal:** Personalized home page with applications, renewals, notifications
- **Public Sector consoles:** Unified staff workspace for review and approvals
- **Mobile-first design:** Touch-optimized with offline capability
- **State branding:** Consistent visual identity throughout

Application Tracking:

Real-time visibility into application progress:

- **Visual progress:** Path showing stages (Draft → Submitted → Under Review → Approved → Issued)
- **Status updates:** Current position, pending actions, missing documentation
- **Automated notifications:** Email/portal alerts for status changes
- **Timeline view:** Chronological actions with timestamps
- **Estimated completion:** Predictive analytics based on historical data
- **Document upload:** Drag-and-drop with validation
- **Payment tracking:** History, outstanding fees, receipts
- **Communication log:** All correspondence in one place

Multi-Permit Application:

Streamlined process for applying to multiple permits:

- **Single identity:** Unified profile with contact details, payment preferences, history
- **Pre-populated forms:** Autofill known fields from existing data
- **Document reuse:** Attach previously uploaded files to new applications
- **Consolidated dashboard:** All applications with quick actions (Apply, Renew, Modify)
- **Smart recommendations:** Suggest related permits
- **Batch submission:** Multiple permits in single session
- **Cross-application visibility:** Staff see complete permit portfolio

Guided Workflows:

Step-by-step assistance through complex applications:

- **Interactive wizards:** OmniScript flows with progress indicators
- **Conditional logic:** Dynamic forms adapting to responses
- **Contextual help:** Tooltips and explanations at each step
- **Auto-save:** Every 30 seconds preventing data loss
- **Real-time validation:** Error checking before submission
- **Review summary:** Final verification screen

Self-Service Features:

Empowering users to manage permits independently:

- **Portfolio view:** All permits/licenses in one location
- **Renewal reminders:** 90/60/30-day alerts with one-click renewal
- **Online modifications:** Address updates, ownership transfers
- **Digital permits:** PDF downloads with QR codes
- **Payment management:** Update methods, view history, payment plans
- **24/7 support:** AI chatbot and live chat during business hours

Accessibility:

Ensuring inclusive access for all users:

- **Screen reader support:** Semantic HTML and ARIA labels
- **Keyboard navigation:** Full functionality without mouse
- **WCAG AA contrast:** Compliant text and element ratios
- **Plain language:** 8th-grade reading level
- **Bilingual:** English and Spanish throughout
- **Video tutorials:** Embedded how-to guides

Example User Journey:

1. Login with SSO → Dashboard shows existing food service permit
2. Click "Apply for Additional Permit" → Outdoor Seating Authorization
3. Form auto-fills business information from profile
4. Reattach insurance certificate from prior application
5. Upload new site plan
6. Review, pay, submit → Receive confirmation with timeline
7. Track progress → Receive approval → Download combined permit

IBM's interface enables transparent application tracking, efficient multi-permit submissions using saved data, and modern digital interaction—reducing processing time, eliminating redundant entry, and improving satisfaction while meeting all statutory and accessibility requirements.

4.2.1.4 Vendors should describe how the solution assists public users through the application process, the vendor should implement an intelligent, interactive assistant (AI) or automated tool embedded within the public dashboard.

IBM's proposed solution integrates an **AI driven, interactive assistant** within the **Salesforce Experience Cloud public dashboard** to help constituents navigate the permitting and licensing process with ease. This assistant - powered by **Salesforce Einstein capabilities** - will provide step-by-step guidance, contextual information, and real time responses to user questions.

The result is a **personalized, conversational experience** that simplifies complex processes, reduces errors, and increases completion rates for online applications while lowering support demands on the Agency's staff.

Purpose and Vision

The interactive assistant is designed to:

- **Guide applicants** through each stage of the application process using natural language dialogue.
- **Answer common questions** (e.g., eligibility criteria, required documents, payment methods).
- **Recommend next steps** based on where the user is in the workflow.
- **Proactively alert users** to missing information or approaching deadlines.
- **Connect users to live support** when inquiries require human assistance.

This approach aligns with IBM's vision of **human-centered digital government**, where AI and automation simplify access to public services and enable equitable experiences for all users.

4.2.1.5 Vendors should explain how the solution would implement a dynamic and transparent tracking system within the public dashboard that would provide public users with up-to-date visibility into the status and progress of their applications throughout the approval workflow.

IBM's solution implements a dynamic tracking system within the public dashboard providing real-time visibility into application status and progress. Built on Salesforce Experience Cloud, the dashboard automatically updates as applications move through stages, displaying visual progress indicators, timestamps, milestones, and next-step guidance with instant synchronization to back-office processing.

Real-Time Status Display:

Visual indicators provide at-a-glance understanding of application progress:

- **Progress tracker:** Path showing stages (Submitted → Under Review → Inspection → Approved → Issued)
- **Percentage complete:** Progress bar indicating workflow advancement
- **Status labels:** Plain-language descriptions ("Under Technical Review," "Awaiting Payment")
- **Automatic updates:** Instant refresh when agency staff take actions
- **Color-coded indicators:** Green (on track), yellow (action needed), red (issue/delay)

Timeline and Milestones:

Chronological view of all application activity:

- **Event timeline:** Date, time, description for all actions
- **Milestone markers:** Key checkpoints highlighted (Application Complete, Inspection Passed)
- **Elapsed time:** Days since submission and at current stage
- **Estimated completion:** Predicted approval date from historical data
- **Deadline countdown:** Days remaining until statutory deadline

Communication Log:

Complete transparency of all interactions:

- **Activity tracking:** Every action logged (document uploaded, reviewer assigned, payment received)
- **Agency notes:** Reviewer comments visible to applicant

- **Two-way messaging:** In-app communication between applicant and staff
- **Document activity:** Upload, review, approval status tracking
- **Payment history:** All transactions and receipts

Notifications and Guidance:

Proactive alerts keeping applicants informed:

- **Automated alerts:** Email/SMS for status changes and deadlines
- **Action flags:** Dashboard highlights required responses
- **Next steps:** Clear instructions for applicant actions
- **Renewal reminders:** Proactive expiration notifications

Multi-Application Management:

Unified view of all permits and licenses:

- **Portfolio view:** Active, pending, approved, historical applications
- **Filtering/sorting:** Organize by status, date, type, agency
- **Quick actions:** Upload, pay, contact, renew buttons
- **Related permits:** Connections between associated applications

Document and Payment Tracking:

Detailed visibility into requirements and finances:

- **Document checklist:** Complete/incomplete status with upload links
- **Review status:** Track when documents approved
- **Fee breakdown:** Itemized paid, outstanding, refunded amounts
- **Payment methods:** Stored methods and transaction history
- **Digital receipts:** Download/print capability

Mobile Access:

Full functionality on any device:

- **Mobile-optimized:** Complete tracking on smartphones/tablets
- **Push notifications:** Real-time alerts (with mobile app)
- **QR code login:** Simplified mobile access

Inspection Management:

Scheduling and results visibility:

- **Appointments:** Date, time, inspector, location
- **Calendar integration:** One-click calendar addition
- **Results:** Pass/fail with photos and notes
- **Re-inspection:** Request follow-up if needed

Technical Implementation:

Salesforce-native capabilities enable reliability:

- **Case object:** Applications tracked with automatic status updates
- **Flow automation:** Workflow rules trigger changes and notifications
- **Lightning components:** Custom progress and timeline displays
- **Platform Events:** Real-time back-office/portal synchronization
- **CRM Analytics:** Predictive completion dates

Transparency Features:

Building trust through openness:

- **Reviewer identity:** Name and contact visible
- **Benchmarks:** Actual vs. average processing time
- **Delay explanations:** Clear reasons for any delays
- **Appeal information:** Instructions and deadlines if denied
- **Public records:** Searchable approved permits

Accessibility:

Ensuring inclusive access:

- **Plain language:** Jargon-free descriptions
- **Visual hierarchy:** Important information prominent
- **WCAG 2.2 AA:** Full assistive technology support
- **Bilingual:** English and Spanish throughout
- **Printable:** PDF status summaries

IBM's tracking system provides complete application visibility, eliminates uncertainty through real-time updates, reduces status inquiry calls, builds public trust through transparency, and enables statutory deadline compliance—making timelines visible to both applicants and agencies.

4.2.1.6 Vendors should explain how the solution will implement a robust session management and draft-saving system for mid-process applications.

IBM's solution implements secure session management and automatic draft-saving preventing data loss from timeouts, network interruptions, or information-gathering pauses. The system uses SSO authentication with encrypted tokens, configurable timeouts, and automatic warnings. Draft-saving stores user input continuously, allows manual saves at any point, and enables seamless resumption exactly where users left off.

Session Management:

Secure, flexible session controls balance security with usability:

- **SSO authentication:** SAML 2.0/OpenID Connect with State identity management
- **Encrypted tokens:** TLS 1.3 with auto-invalidation on logout/timeout
- **Configurable timeouts:** 15 minutes (public), 30 minutes (staff)
- **Timeout warnings:** 2-minute alert with extension option
- **Activity-based extension:** User actions reset timeout clock
- **Multi-device support:** Resume across desktop, tablet, smartphone
- **Concurrent session control:** Prevent unauthorized simultaneous access
- **Auto-recovery:** Restore state after unexpected disconnection
- **Token refresh:** Background renewal for long sessions

Automatic Draft-Saving:

Continuous data preservation without user intervention:

- **Auto-save frequency:** Every 30 seconds, on field update, navigation, or step completion
- **Silent operation:** Background saves without workflow interruption
- **Draft records:** Stored with "Draft" status in Salesforce
- **Zero data loss:** Preserved through browser crashes or network failure
- **Local backup:** Encrypted browser cache for redundancy

Manual Save Options:

User-controlled save capability:

- **"Save and Exit" button:** Explicit save with confirmation
- **Save anywhere:** Available at every application step
- **Email confirmation:** Optional notification with resume link

Draft Management:

Easy access and organization of saved work:

- **Dashboard listing:** All drafts with permit type, save date, completion percentage
- **One-click resume:** Reopen at exact saved step with pre-populated data
- **Progress indicators:** Completed and remaining sections displayed
- **Multiple drafts:** Concurrent drafts for different permit types
- **Edit capability:** Modify information before submission

Data Protection:

Security and integrity controls:

- **AES-256 encryption:** All draft data encrypted at rest
- **Access control:** RBAC enables only creators can access
- **Session binding:** Edits only within authenticated session
- **Automatic purge:** Deleted when user account closed
- **Private drafts:** Not visible to agency staff until submitted

Validation and Retention:

Balancing flexibility with data integrity:

- **Flexible saving:** Drafts saved regardless of completeness
- **Submission validation:** Full validation required before final submit
- **Inline checking:** Real-time error detection during entry
- **90-day retention:** Configurable by agency policy
- **Expiration warnings:** Notifications at 14, 7, 1 days before deletion
- **Archival process:** Expired drafts archived before purging

Mobile and Cross-Device:

Seamless experience across platforms:

- **Mobile access:** Full management on smartphones/tablets
- **Offline drafts:** Local save when no network, sync on reconnection
- **Cross-device sync:** Start desktop, continue mobile, complete tablet

User Experience:

Intuitive progress tracking and recovery:

- **Visual indicators:** Status badge, timestamp, auto-save spinner
- **Breadcrumb navigation:** Current position in multi-step form
- **Field persistence:** Text, dropdowns, uploads, signatures supported
- **Document retention:** Uploaded files saved with draft
- **Deferred payment:** Complete application details, pay later

Example Flow:

1. Start permit application → Complete Section 1
2. Need documents → Click "Save and Exit"
3. Return days later → Login shows "Draft - 60% complete"
4. Click "Resume" → Opens at Section 2 with Section 1 intact
5. Complete, upload, submit → Validates and processes

IBM's system provides flexible completion pacing without data loss, reduces abandonment through accommodation of information-gathering breaks, improves quality through thoughtful completion, enhances satisfaction via seamless multi-device experience, and maintains security through encryption and access controls.

4.2.1. 7 Vendors should describe how the solution implements a transparent and dynamic time-tracking module within the public dashboard.

IBM's time-tracking module provides real-time visibility into application processing, displaying visual timelines, elapsed days, milestones, and estimated completion dates with automatic updates as agency staff act. This capability is statutorily mandated—West Virginia's permitting reform legislation requires agencies to process applications within specific timeframes or automatically refund fees charged to the responsible agency's budget. The tracking increases public trust, reduces inquiries, and enables accountability.

Visual Timeline:

Clear display of workflow progress:

- **Stage-by-stage path:** Submitted → Under Review → Inspection → Approved → Issued
- **Milestone markers:** Date/time achieved and SLA target for each stage
- **Color indicators:** Green (on track), yellow (in progress), red (overdue/at risk)
- **Progress percentage:** Overall completion through approval process

Real-Time Counters:

Dynamic metrics updating instantly:

- **Elapsed time:** Days since submission with timestamp
- **Stage duration:** Time at current workflow stage
- **Estimated completion:** Predicted date from historical averages
- **Deadline countdown:** Days remaining; visual alert when approaching
- **Instant refresh:** Updates when staff act—no delays

Milestone Details:

Comprehensive action information:

- **Action details:** Who, when, what happened (hover/click)
- **Next steps:** Clear indication of requirements
- **Waiting status:** Display if agency awaits documentation/review
- **Responsible party:** Current reviewing agency/department

Statutory Deadline Enforcement:

Compliance with refund requirements:

- **10-day completeness:** Countdown for agency response
- **Cure period:** 30-day applicant response with paused main deadline
- **Refund warnings:** Clear alerts when approaching deadline
- **Financial transparency:** Refund amount and processing date

Notifications:

Proactive communication:

- **Automated alerts:** Email/SMS for milestones and changes
- **Deadline warnings:** 75%, 90%, 100% of allowed time
- **Action flags:** Prominent when response needed
- **Completion notices:** Immediate approval/denial notification

Historical Tracking:

Complete activity record:

- **Audit trail:** Chronological log with timestamps
- **Document activity:** Upload, review, approval tracking
- **Communication log:** All applicant/agency messages
- **Payment history:** Fees, refunds, balances

Agency Accountability:

Public performance visibility:

- **SLA comparison:** Actual vs. published targets
- **Performance transparency:** Public view of deadline compliance
- **Reviewer identification:** Staff name and contact
- **Escalation visibility:** Supervisor involvement indicator

Technical Implementation:

Salesforce-native automation:

- **Flow automation:** Status updates and time calculations
- **Platform Events:** Real-time back-office/portal sync
- **Lightning components:** Interactive timeline visualization
- **CRM Analytics:** Predictive completion dates
- **Apex triggers:** Elapsed time and refund calculations

Mobile Access:

Full functionality anywhere:

- **Responsive design:** Complete features on all devices
- **Touch-optimized:** Easy mobile interaction
- **WCAG 2.2 AA:** Full accessibility support
- **Push notifications:** Real-time mobile alerts

IBM's time-tracking module enables statutory compliance, provides complete visibility, reduces status inquiries, promotes accountability through public deadline tracking, and builds trust through real-time transparency, transforming a legal mandate into operational excellence.

4.2.1.8 Vendors should explain how the proposed solution implements a mobile-friendly, offline-capable inspection module that allows field inspectors to work seamlessly without network connectivity, then queue those for automatic upload once connected to a network.

IBM's Inspection Management module provides native iOS/Android applications enabling field inspectors to complete entire workflows without network connectivity. The system automatically detects connectivity loss and transitions seamlessly to offline mode, storing all data locally with FIPS 140-3 encryption. When connection is restored, changes automatically queue for upload

without manual intervention, eliminating data loss and ensuring continuous productivity regardless of network availability.

Native Mobile Applications:

Purpose-built apps optimized for field operations:

- **iOS and Android apps:** Superior performance versus browser-based solutions
- **Automatic offline mode:** Seamless transition without workflow interruption
- **Complete field functionality:** View assignments, permit details, site plans, documents; GPS navigation; full inspection execution offline

Field Data Collection:

Comprehensive tools for inspection documentation:

- **Smart checklists:** Permit-specific with pass/fail/N/A options, conditional logic, mandatory fields
- **Media capture:** Photos/videos with automatic GPS geotagging, timestamps, annotation tools, multiple images per item
- **Voice-to-text:** Speech recognition for faster note-taking
- **Digital signatures:** On-site capture from property owners/contractors with legal validity

Data Management:

Secure storage and intelligent synchronization:

- **Encrypted storage:** All local data secured meeting FIPS 140-3 standards
- **Intelligent sync:** Auto-detects network restoration, queues uploads, prioritizes critical data
- **Background sync:** Uploads occur while inspector continues working
- **Bandwidth optimization:** Text syncs immediately; large files deferred for stronger connection
- **Conflict resolution:** Configurable rules for simultaneous edits (inspector update typically prevails)
- **Instant updates:** Synced results immediately appear in permit record triggering workflows

Security and Compliance:

Enterprise-grade protection for mobile devices:

- **Device authentication:** PIN/biometric access control
- **Auto-timeout:** Automatic session expiration preventing unauthorized access
- **Remote wipe:** Lost/stolen device data erasure capability
- **Complete audit trail:** All actions logged with timestamps, GPS coordinates, inspector attribution
- **Sync policies:** Configurable time limits (e.g., end-of-day) ensuring freshness

Performance and Coordination:

Optimized for all-day field use:

- **Hardware acceleration:** Efficient memory management and battery optimization
- **Multi-inspector coordination:** Prevent duplicate assignments; real-time reassignments when connected
- **All-day battery:** Performance optimized for extended field operations

IBM's offline-capable inspection module enables efficient work regardless of connectivity, increases daily inspection volume with higher accuracy, eliminates paperwork and manual

entry, and provides immediate results to applicants—accelerating permit processing while maintaining complete regulatory compliance.

4.2.1.9 Vendors should explain how the solution is accessible with mobile devices for both public and agency users, the system should be designed with an approach that ensures full functionality, usability, and performance across mobile devices such as smartphones and tablets.

IBM delivers a mobile-responsive, fully accessible permitting solution built on Salesforce Public Sector Solutions with native cross-device compatibility. The Salesforce Lightning framework and Experience Cloud provide consistent functionality across smartphones, tablets, and desktops for both public users and agency staff—enabling application submission, review, workflow management, and communication from any device with the same security and performance as desktop systems.

Mobile-First Design Approach:

IBM's Enterprise Design Thinking methodology enables intuitive, responsive interfaces:

- **Mobile-first layouts:** Dynamic adaptation to all screen sizes using Lightning Components
- **Responsive design:** HTML5/CSS3 automatic resizing and content reflowing
- **Touch-friendly navigation:** Buttons, menus, fields optimized for finger interaction
- **Progressive disclosure:** Complex tasks broken into clear stages with contextual guidance
- **Offline capability:** Field staff view, edit, sync records without connectivity
- **WCAG 2.2/Section 508 compliance:** Iterative testing with users and accessibility experts

Public User Mobile Experience:

Citizens and businesses access the portal via standard mobile browsers or Salesforce Mobile App:

- **Apply and pay:** Complete applications, upload documents, process payments on mobile-friendly forms
- **Track and receive alerts:** Status updates, reminders optimized for mobile display via email/push notifications
- **Document capture:** Camera integration for photos and document scanning with direct attachment
- **Accessibility:** Readable text, color contrast, navigation for smaller screens; assistive technology support
- **Adaptive performance:** Cloud architecture maintains fast load times on mobile networks
- **Browser-based access:** No specialized software required; secure HTTPS with multi-factor authentication

Agency Staff Mobile Experience:

Internal staff use Salesforce Mobile App and mobile-optimized Public Sector Solutions Console:

- **Application management:** Review submissions, approve/reject, assign tasks from smartphones/tablets
- **Field inspections:** Capture photos, update findings, record notes offline; automatic sync when connected
- **Calendar integration:** Outlook/Google Calendar access for inspections and meetings
- **Dashboard access:** Mobile-responsive charts and reports via CRM Analytics
- **Push notifications:** Urgent case alerts and appointment changes

Technology Enablers:

Platform components supporting mobile functionality:

- **Lightning Framework:** Responsive design auto-adjusting for screen sizes
- **Experience Cloud:** Browser-based public access without additional software
- **Salesforce Mobile App:** Native iOS/Android with offline and push notifications
- **Platform Encryption:** Secure mobile transactions (data at rest and in transit)
- **MuleSoft integration:** Connect payment processors, address verification, calendars
- **CRM Analytics:** Interactive mobile dashboards and reports

Mobile Security:

Enterprise-grade protection for mobile access:

- **SSO integration:** SAML 2.0/OpenID Connect with State identity provider
- **Multi-factor authentication:** Required for internal and external users
- **Session management:** Mobile-specific policies preventing unauthorized access during idle periods
- **Role-based access:** Mobile data visibility restricted by user role
- **FedRAMP High:** Government Cloud authorization ensuring cybersecurity compliance

Performance Optimization:

Strategies maintaining high mobile performance:

- **Cloud-native scalability:** Automatic resource scaling for mobile traffic fluctuations
- **Content Delivery Network:** CDN serving static assets for faster load times
- **Adaptive rendering:** Lightweight techniques for dashboards and charts on mobile browsers
- **Caching and compression:** Local caching in mobile app minimizing network load
- **Monitoring and analytics:** Track usage metrics; optimize load times and navigation paths

IBM's mobile-responsive solution provides consistent, high-performance access across all devices, enabling citizens to complete permitting tasks anywhere while empowering field staff with offline-capable tools—all within a secure, accessible, FedRAMP-compliant environment ensuring operational continuity regardless of location or device.

4.2.1.10 Vendors should describe how the solution implements a flexible and user-controlled notification system. The system should allow users to be able to sign up for and receive workflow notifications throughout the process through email, mobile phone, or both as the individual chooses.

IBM's notification system empowers users to customize how, when, and where they receive workflow alerts and updates. Within the Experience Cloud portal, users manage notification preferences directly from their profile, selecting delivery channels—email, SMS, or both—based on personal preference. Salesforce Flow Builder triggers automated alerts for key events including submission confirmation, completeness determinations, payment reminders, status changes, inspection scheduling, and renewal deadlines. This approach enables personalized, transparent communications under user control while maintaining privacy, accessibility, and security compliance.

Multi-Channel Delivery:

Flexible communication options meeting user preferences:

- **Channel selection:** Email, SMS, or both with different channels for different notification types
- **Self-service management:** Intuitive toggle controls on profile page, no staff assistance needed

- **Granular controls:** Opt in/out of specific categories (status updates, payments, documents, inspections, approvals, renewals, maintenance, policy changes)
- **Real-time triggers:** Flow automation generates notifications immediately when events occur
- **Personalized content:** Permit type, application number, status, action required, deadline, portal link, agency contact
- **Mobile-optimized:** Concise SMS for mobile; responsive HTML email for all devices
- **Frequency controls:** Immediate, daily digest, or weekly summary options
- **Timing preferences:** Business hours only or any time
- **Instant updates:** Preference changes take effect immediately

Security and Compliance:

Protected, compliant communications:

- **Consent management:** Clear records with opt-out in every message; CAN-SPAM/TCPA compliant
- **Secure delivery:** Encrypted SMTP with SPF/DKIM/DMARC; FedRAMP-authorized SMS gateway
- **Multi-language:** English and Spanish based on profile preference
- **Accessibility:** Alt text, semantic HTML, high-contrast meeting WCAG 2.2 AA
- **Delivery tracking:** Log all attempts with status (sent, delivered, bounced, failed)
- **Fallback mechanisms:** SMS failure triggers email; bounced email flags for update
- **Audit trail:** Timestamp, recipient, channel, content, status logged
- **Opt-out compliance:** Remove from non-essential while maintaining legally required notices

Advanced Features:

Enhanced functionality and reliability:

- **Push notifications:** Optional mobile app provides in-app real-time alerts
- **Agency staff controls:** Internal notification preferences for assignments, escalations, deadlines
- **Notification templates:** Pre-configured, legally reviewed ensuring consistency
- **Scalability:** Enterprise infrastructure with throttling and queuing for high-volume scenarios
- **Testing capability:** Send test notifications to verify delivery and format

Example Notifications:

- **Submitted:** "Your [Type] application #[Number] received. Est. time: [Days]. Track: [Link]"
- **Action needed:** "Additional documents required for #[Number]. 30 days to respond. Upload: [Link]"
- **Inspection:** "Site inspection [Date] at [Time]. Inspector: [Name]. Questions? [Phone]"
- **Approved:** "Congratulations! [Type] #[Number] approved. Download: [Link]"
- **Renewal:** "[License] expires in [Days]. Renew now: [Link]"
- **Refund:** "Application #[Number] exceeded deadline. Refund $[Amount] issued."

IBM's notification system keeps applicants informed, reduces status inquiry calls, improves satisfaction through transparency and control, enables deadlines aren't missed, and maintains full communication regulation and accessibility compliance—demonstrating West Virginia's commitment to customer-centric government service.

4.2.1.11 Vendors should explain how the solution includes a flexible, secure, and user-friendly form and document management module with the ability to upload documents or create fillable forms for certain permits as needed.

IBM's form and document management module supports both public users and agency staff throughout the permitting process. Built on Salesforce Files and Content Management, extended through OmniStudio and Intelligent Document Automation, the system enables users to upload documents, complete fillable forms, and securely associate files with applications. OmniScript-based digital forms guide users step-by-step, auto-populate known data, and support e-signature integration with DocuSign or Adobe Sign. Agency administrators create or modify templates using low-code tools ensuring flexibility without custom development.

Document Upload:

Intuitive, secure document submission:

- **Drag-and-drop interface:** Upload on desktop, tablet, mobile via drag-and-drop or file browser
- **Format support:** PDF, Word, Excel, images, CAD files (.dwg, .dxf), ZIP archives
- **File size limits:** Configurable limits; supports up to 2GB for engineering drawings
- **Virus scanning:** Real-time enterprise antivirus with infected file quarantine
- **Categorization:** Assign to categories (insurance, site plan, assessment) ensuring proper routing
- **Batch upload:** Multiple simultaneous uploads reducing submission time
- **Mobile camera:** Direct capture and upload with automatic optimization
- **Progress indicators:** Real-time bars with time estimates; cancel/retry capability
- **Version control:** History of updates/replacements with audit trail
- **Reordering:** Drag-and-drop document organization

Fillable Forms:

Dynamic, intelligent forms streamlining data entry:

- **OmniScript-powered:** Guided step-by-step entry with conditional logic
- **Auto-population:** Pre-fill from profile, prior applications, integrated sources
- **Real-time validation:** Immediate error feedback with correction guidance
- **Save-as-draft:** Resume later; auto-save every 30 seconds
- **Multi-page with progress:** Logical sections with completion percentage
- **Responsive design:** Optimal layout on desktop, tablet, smartphone
- **WCAG 2.2 AA:** Screen reader compatible, keyboard navigation, clear labels
- **Contextual help:** Tooltips, FAQs, support links at each field
- **E-signature:** DocuSign/Adobe Sign integration for legal binding
- **Automatic calculations:** Fees, totals, derived values computed
- **Dynamic fees:** Based on permit type, project value with transparent breakdown
- **Bilingual:** English and Spanish with mid-session toggle

Administrator Tools:

Low-code configuration empowering agency staff:

- **Form builder:** Drag-and-drop field placement, conditional logic, validation rules without programming
- **Template library**: Pre-built common permit forms customizable to agency needs
- **Document checklists:** Define required documents, formats, mandatory/optional status
- **Version management:** Track versions, deploy updates, maintain backward compatibility
- **Preview and testing:** View as end users before publication
- **Approval workflows:** Internal review ensuring legal/policy compliance

Security and Compliance:

Enterprise-grade protection:

- **AES-256 encryption**: At rest and TLS 1.3 in transit meeting FIPS 140-3
- **FedRAMP High:** Government Cloud storage with federal controls
- **Role-based access:** Visibility controlled by user role
- **Audit trails:** Complete logging (upload, view, download, modification, deletion)
- **Retention policies:** Automated archival/purging per State records policy
- **Redaction:** Authorized staff remove sensitive information
- **Watermarking:** Optional user identity and timestamp on downloads

Review and Collaboration:

Efficient agency workflows:

- Inline viewer: Review without downloading supporting common formats
- Annotation tools: Comments, highlights, stamps, markups
- Document checklists: Mark reviewed, approved, or needs revision
- Request documents: Automated notifications with specific instructions
- Version comparison: Side-by-side highlighting changes
- Inter-agency sharing: Permission-controlled access for multi-department reviews

Integration:

Seamless connectivity:

- **Legacy sync:** Automatic synchronization to agency systems via MuleSoft/APIs
- **GIS integration:** Link site plans to coordinates for map visualization
- **OCR capability:** Extract data from PDFs/images auto-populating fields
- **Digital signatures:** DocuSign/Adobe Sign with certificates and audit trails
- **Export packages:** Complete applications as ZIP for offline storage

IBM's module streamlines submissions, reduces errors through validation and auto-population, accelerates reviews with inline tools, enables security through encryption and access controls, and empowers agencies to adapt quickly using low-code configuration—eliminating paper inefficiencies and delivering superior experiences.

4.2.1.12 Vendors should demonstrate strategic implementation of the tool for both agencies and public users, vendors should showcase their ability to seamlessly integrate with existing portals and permitting systems while enhancing functionality, accessibility, and user experience.

IBM demonstrates strategic implementation seamlessly integrating with existing state portals and permitting systems while enhancing functionality, accessibility, and user experience. The solution interoperates with current technologies through flexible strategies using MuleSoft Anypoint Platform, Salesforce-native APIs, and open standards—ensuring existing data sources, authentication systems, payment processors, and legacy databases remain operational while new services are introduced without disruption.

Integration with State Infrastructure:

Seamless connectivity preserving existing investments:

- **SSO integration:** SAML 2.0/OpenID Connect with State identity management eliminating separate credentials
- **State portal embedding: Experience** Cloud embedded in wv.gov or standalone with consistent branding
- **Legacy connectivity:** Bidirectional integration across seven departments using REST/SOAP APIs, database connectors, or file-based methods

- **Payment gateway:** State-approved processor connection without changing accounts, contracts, or reconciliation
- **Accounting integration:** Automated posting of fees, refunds, cost allocations to ERP systems
- **GIS integration:** County and state GIS connection for map-based applications and site verification
- **Document repository:** Interface with existing management systems maintaining archival practices
- **Communication systems**: State email servers and SMS gateways maintaining policy compliance
- **Calendar systems:** Inspection scheduling, hearings, appointments

Functionality Enhancement:

Transformative capabilities beyond current systems:

- **Unified registry:** Consolidate seven departments into single master registry eliminating silos
- **Cross-agency visibility:** Complete applicant history across all departments
- **Automated routing:** Replace manual handoffs with intelligent workflow automation
- **Deadline enforcement:** Statutory refund requirements through automated monitoring and triggering
- **Fast-track processing:** Optional expedited permitting with dynamic fee calculation
- **Real-time analytics:** Processing trends, workload distribution, bottleneck identification
- **Mobile inspections:** Offline-capable app replacing paper with digital checklists, photos, GPS
- **Collaboration tools:** Messaging, shared notes, coordinated reviews replacing email chains
- **Predictive analytics:** AI-driven forecasting and risk identification

User Experience Enhancement:

Modern, accessible interfaces for all users:

- **WCAG 2.2 AA:** Screen reader compatibility, keyboard navigation, color contrast optimization
- **Mobile-responsive:** Auto-adapt to desktop, tablet, smartphone
- **Plain language:** Jargon-free instructions understandable to general public
- **Bilingual:** English and Spanish throughout
- **Guided workflows:** Step-by-step wizards with progress indicators
- **Auto-population**: Pre-fill from profile, prior applications, integrated sources
- **Status transparency**: Visual timeline with progress, elapsed time, next steps
- **Self-service:** Upload, pay, track, download without staff contact
- **AI chatbot:** 24/7 assistance reducing call volume
- **Personalized dashboards:** Customized views by user

Agency Experience Improvement:

Optimized tools for staff productivity:

- **Role-based** dashboards: Tailored for reviewers, inspectors, supervisors, executives
- **Intelligent queues:** Auto-sorted by urgency with visual indicators
- **360-degree view:** Complete history eliminating multi-system checks
- **Inline document tools:** Review, zoom, annotate without downloading
- **One-click actions:** Streamlined approvals with templates and audit trails

- **Mobile field tools:** Offline-capable smartphone/tablet access
- **Collaboration features:** Internal messaging, @mentions, shared notes
- **Performance analytics:** Team productivity monitoring and optimization
- **Self-service admin:** Low-code configuration without IT support

Demonstration Approach:

Concrete evidence of capability:

- **Live walkthrough:** Interactive public portal and agency dashboards with realistic scenarios
- **Integration showcase:** SSO, payment, data sync, document upload in real-time
- **Accessibility demo:** Screen reader, keyboard-only, mobile compliance
- **Workflow simulation:** End-to-end application through review, inspection, approval
- **Analytics display:** Operational metrics, financial performance, strategic insights
- **Mobile capabilities:** Field inspection with offline capture and sync
- **Administrative tools:** Low-code permit type creation and form modification
- **Comparative analysis:** Current vs. future-state efficiency gains

Strategic Value:

Long-term benefits for West Virginia:

- **Faster implementation:** Configuration-first approach meeting January 1, 2027 deadline
- **Lower TCO:** Cloud SaaS eliminating infrastructure costs; low-code reducing maintenance
- **Reduced dependency:** State staff empowered for independent configuration
- **Continuous innovation:** Three annual Salesforce updates at no additional cost
- **Scalability:** Accommodate additional agencies, permits, volumes without replacement
- **Proven track record:** Hundreds of successful state/local implementations
- **Risk mitigation:** Hybrid Agile, phased approach with continuous testing and feedback

Future Integration & Platform Options:

During the initial implementation, IBM will leverage Salesforce's native API and integration capabilities to meet all required connectivity and data-exchange needs. As the program matures, MuleSoft Anypoint Platform can be introduced to extend enterprise-level integration across additional agencies or high-volume systems. IBM will collaborate with the State during the Discovery Phase to finalize detailed integration requirements, interface volumes, and architectural decisions regarding MuleSoft adoption.

IBM's approach delivers seamless integration preserving State investments while introducing transformative capabilities, achieving transparency, efficiency, accountability, and satisfaction goals—meeting statutory requirements while positioning West Virginia for digital government excellence.

4.2.1.13 Vendors should demonstrate how their solution would provide effective data security and protection, alongside ongoing support, maintenance, and adjustment of the program and dashboard to meet changing needs.

IBM's solution provides comprehensive data security through Salesforce Government Cloud with FedRAMP High authorization, FIPS 140-3 encryption, multi-factor authentication, and NIST 800-53 compliance. Our Maintenance and Operations framework delivers proactive monitoring, regular updates, security patches, and rapid incident response ensuring maximum uptime and data protection while adapting dynamically to changing operational, regulatory, and service delivery needs.

Data Security and Protection:

Enterprise-grade security controls protect sensitive information:

- **FedRAMP High:** Government Cloud with federal security controls and continuous monitoring
- **FIPS 140-3 encryption:** AES-256 at rest, TLS 1.3 in transit
- **Shield Platform Encryption:** Field-level protection for PII, SSN, payment data with key rotation
- **Multi-Factor Authentication:** Required for all users (TOTP, SMS, authenticator apps)
- **SSO integration:** SAML 2.0/OpenID Connect with State identity system
- **Role-Based Access Control:** Granular permissions enforcing least privilege
- **Session management:** Auto-timeout (15 min public, 30 min staff); IP restrictions for admins
- **Audit logging:** Tamper-proof logs retained seven years
- **Data loss prevention:** Automated export blocking; document watermarking
- **Network security:** WAF protection (SQL injection, XSS, DDoS); intrusion detection/prevention
- **Vulnerability management:** Weekly scanning, annual penetration testing; 72-hour critical fixes
- **PCI-DSS compliance:** Tokenized payment processing; annual validation
- **Data residency:** US-only storage; offshore access prohibited
- **Backup/recovery:** Real-time replication, 4-hour incremental, daily full, 90-day retention
- **24/7 SOC monitoring:** Threat detection; documented incident response; quarterly exercises
- **Privacy protections:** Data minimization, consent management, subject rights support
- **Compliance:** NIST 800-53 Rev 5, State policies; quarterly assessments

Ongoing Support and Maintenance:

Structured support ensuring system reliability:

- **Tiered support:** Tier 1 (8AM-6PM ET), Tier 2 (24/7), Tier 3 (On-Call)
- **SLAs:** Critical (1-hr response, 4-hr resolution), High (4-hr/1-day), Medium (1-day/5-day), Low (2-day/10-day)
- **24/7 monitoring:** Performance, availability, transactions, errors, security with automated alerts
- **Monthly:** Health checks, tuning, patches, feedback review, minor enhancements
- **Quarterly:** Feature releases, usability testing, DR drills, security assessments, business reviews
- **Annual:** Salesforce upgrades (3x/year), roadmap planning, audits, surveys, TCO analysis
- **Change management:** Structured review, impact assessment, sandbox testing, rollback
- **Self-service:** Knowledge base (articles, videos, FAQs); user community
- **Release management:** Coordinated deployments; maintenance windows (Sat 10PM-Sun 6AM) with notice
- **Performance optimization:** Continuous monitoring preventing degradation
- **Capacity planning:** Analysis with forecasting and scaling recommendations

Continuous Enhancement:

Adaptive system evolution:

- **Hybrid Agile enhancements:** Prioritized backlog; 4-6 week delivery cycles
- **User feedback:** Surveys, focus groups, usability testing
- **Configuration flexibility:** Low-code tools for State staff modifications
- **Agency onboarding:** Structured process for adding agencies/permit types
- **Regulatory response:** Rapid legislation adaptation; emergency procedures

- **Integration expansion:** Connect additional systems as needed
- **Analytics evolution:** New dashboards and predictive models
- **AI advancement:** Chatbot improvements; expanded automation
- **Mobile updates:** Regular releases with feedback and OS compatibility
- **Accessibility:** Ongoing WCAG compliance; assistive technology support

Customer Center of Excellence:

Dedicated partnership ensuring success:

- **Dedicated team:** Named IBM resources with West Virginia expertise
- **Knowledge transfer:** State staff training (administration, configuration, troubleshooting)
- **Best practices:** Lessons from implementations; industry trends; innovations
- **Executive reviews:** Quarterly meetings (performance, adoption, metrics, alignment)
- **Annual health check:** Comprehensive assessment with recommendations

Disaster Recovery:

High-availability architecture ensuring continuity:

- **Multi-region deployment:** Automatic failover under 5 minutes
- **Recovery objectives:** RTO 4 hours, RPO 4 hours, max downtime 8 hours
- **Quarterly testing:** DR drills with documented improvements
- **Incident communication:** Status page, automated notifications, 30-min updates, post-incident reports

Disentanglement Plan:

Exit strategy ensuring data portability:

- **Delivery:** Within 6 months (data extraction, knowledge transfer, transition support)
- **Data portability:** Standard formats (JSON, XML, CSV) with metadata
- **No lock-in:** No termination fees, pro-rated refunds, free export, transition assistance
- **Documentation:** Complete architecture, integrations, configurations, procedures

IBM's approach enables platform sustainability, data protection, responsive adaptation, and maximized ROI through proactive monitoring, structured maintenance, and knowledge transfer enabling State self-sufficiency.

4.2.1.14 Vendors should demonstrate a comprehensive, flexible, and secure approach that supports interoperability, minimizes disruption, and enhances operational efficiency.

IBM demonstrates a comprehensive approach combining proven methodologies, modern architecture, and structured change management. Our delivery integrates IBM's WWPMM with Hybrid Agile practices and Enterprise Design Thinking, ensuring structured governance and transparent reporting. The solution leverages Salesforce Public Sector Solutions on Government Cloud with flexible integration, declarative configuration, and FedRAMP High/NIST 800-53 security. Phased implementation minimizes disruption while automated workflows deliver measurable efficiency gains.

Comprehensive Approach:

IBM's structured methodology enables successful delivery:

- **WWPMM framework:** Scope management, risk mitigation, quality assurance, stakeholder communication
- **Sprints:** 2-4 week iterations with continuous feedback
- **Design Thinking:** User-centered design with journey mapping and validation

- **Cross-functional team:** Architects, integration specialists, security experts, business analysts, change managers
- **Transparent governance:** Executive steering, weekly reports, risk tracking
- **Quality gates:** Validation, reviews, testing, acceptance at each phase
- **Knowledge transfer:** Technical and functional training for State staff

Flexibility and Interoperability:

Adaptable architecture supporting State needs:

- **Open standards:** REST/SOAP APIs, SAML 2.0, standard data formats
- **Multiple patterns:** Real-time APIs, event-driven messaging, batch transfers
- **MuleSoft option:** Enterprise integration layer if needed
- **Legacy support:** Mainframe, AS/400, Oracle, SQL Server connectors
- **Declarative development:** State administrators modify workflows without programming
- **Low-code tools:** OmniStudio for rapid form creation/modification
- **Modular design:** Independent component enhancement
- **Auto-scaling:** Performance maintained through volume increases
- **API-first:** All functionality exposed for future integration
- **Version control:** Rollback capability for all configurations

Security and Compliance:

Enterprise-grade protection:

- **FedRAMP High:** Government Cloud with federal security controls
- **NIST 800-53:** Full compliance across all control families
- **FIPS 140-3:** AES-256 at rest, TLS 1.3 in transit
- **Defense in depth:** Multi-layered network, application, data, identity security
- **Zero trust:** Continuous verification, least privilege, microsegmentation
- **Identity management:** State SSO, automated provisioning, RBAC, MFA
- **Data protection:** Field encryption, masking, tokenization, US residency
- **PCI-DSS:** Tokenized payment processing
- **24/7 monitoring:** SOC tracking logs, activity, API traffic
- **Vulnerability management:** Weekly scanning, quarterly penetration testing, 72-hour critical fixes
- **Incident response:** Detection, containment, recovery, analysis
- **Audit logs:** Seven-year retention, compliance reporting

Minimizing Disruption:

Smooth transition approach:

- **Phased delivery:** Discovery → Build → Integration → Testing → Go-Live
- **Parallel operations:** Optional period (Jan-July 2027) with dual systems
- **Sandbox environments:** Separate development, testing, training
- **Phased migration:** Reference data, historical records, active applications
- **Rollback capability:** Version control and backups
- **Off-peak maintenance:** Saturday nights with advance notice
- **Change management:** Communication, sponsorship, champions
- **Train-the-trainer:** 2-3 champions per agency
- **Role-based training:** Targeted curricula by user type
- **Hypercare support:** 24/7 for first 30 days
- **Feedback loops:** Rapid issue identification and remediation

Enhancing Efficiency:

Measurable operational improvements:

- **Workflow automation:** Automated routing, notifications, escalations
- **Deadline enforcement:** Countdown timers, alerts, automatic refunds
- **Intelligent queues:** Priority sorting and workload balancing
- **Self-service:** 40-60% call reduction through online capabilities
- **Mobile inspections:** 30-50% administrative time reduction
- **Inter-agency collaboration:** Shared visibility and coordinated workflows
- **Payment automation:** Online collection, instant confirmation, accounting integration
- **Real-time dashboards:** CRM Analytics with drill-down analysis
- **Predictive analytics:** AI-driven risk identification
- **Performance metrics:** KPI tracking (processing times, approval rates, satisfaction)
- **Bottleneck identification:** Analytics highlighting delays
- **Automated reporting:** Scheduled and self-service reports
- **AI chatbot:** 30-40% help desk volume reduction

IBM's approach delivers seamless infrastructure integration, rapid adaptation through low-code configuration, enterprise security, minimal disruption, and enhanced efficiency—ensuring statutory compliance, operational excellence, and citizen satisfaction.

4.2.1.15 Vendors should provide a clear, strategic recommendation regarding integration vs. replacement of existing agency systems, along with a realistic implementation timeline that aligns with the statutory deadline outlined in W.Va. Code §5A-13-I et seq., which mandates full implementation of the One-Stop-Shop Permitting Program by **January 1, 2027.**

IBM recommends a hybrid approach balancing integration of functional agency systems with replacement of outdated or inefficient platforms, determined through a comprehensive discovery assessment. This strategy preserves recent investments while modernizing processes, minimizing disruption, and meeting the January 1, 2027 statutory deadline. Our phased 13-month implementation timeline begins with discovery and agency assessment (Months 1-3), proceeds through platform configuration and integration (Months 4-10), conducts rigorous testing and training (Months 10-12), and culminates in production go-live by January 1, 2027 (Month 13), followed by an optional use transition period through July 1, 2027 when dashboard becomes mandatory.

Integration vs. Replacement Decision Framework:

- **Integrate existing systems when:** System is modern and well-maintained, provides specialized functionality unavailable in Salesforce, represents recent significant investment, agency strongly prefers current system, integration costs are lower than replacement costs
- **Replace with Salesforce when:** System is legacy/near end-of-life, high maintenance costs burden agency budgets, poor user experience hinders productivity, data quality issues compromise accuracy, integration costs exceed replacement costs, consolidation opportunity exists across multiple agencies
- **Assessment criteria:** System age and technology currency, maintenance and support costs, user satisfaction scores, data quality and accessibility, integration complexity and cost, agency readiness for change, statutory compliance capabilities
- Preliminary Agency Recommendations (Validated During Discovery):
  - **Commerce:** Integrate existing business registration database; replace manual permit tracking

- **Environmental Protection:** Integrate specialized environmental modeling tools; replace outdated permit tracking systems
- **Environmental Health Services:** Assess during discovery phase
- **Revenue:** Integrate tax systems; replace manual licensing processes
- **Tourism:** Full replacement recommended (most systems outdated)
- **Transportation:** Integrate inspection scheduling systems; replace paper-based processes
- **Secretary of State:** Integrate corporate filings database

Implementation Timeline (Contract Award December 2025 = 13 Months to January 1, 2027):

- **Phase 1: Discovery & Requirements (Months 1-3 | Dec 2025 - Feb 2026)**
  - Week 1-2: Project kickoff, team mobilization, governance establishment
  - Week 3-6: Stakeholder workshops with all seven departments documenting workflows, permit types, and requirements
  - Week 7-9: Legacy system assessment evaluating integration vs. replacement for each agency
  - Week 10-12: Requirements documentation, architecture design, integration specifications, data migration planning
  - **Deliverable:** Requirements document, system architecture, integration/replacement recommendations, project plan

At the conclusion of Phase 1 "Discovery & Requirements" and before the start of Phase 2 "Platform Configuration" IBM will re-estimate the labor and charges for the subsequent project phases based on the final documented requirements. If the recalculated labor or charges estimates change by more than 10% (increase or decrease) from the planned baseline then IBM will prepare a Contract Change that both parties must sign before proceeding to Phase 2. If the parties can not agree on the Contract Change then either party may terminate the Contract with 5 days notice and without any penalty.

- **Phase 2: Platform Configuration (Months 4-7 | Mar - Jun 2026)**
  - Month 4: Salesforce Government Cloud provisioning, security baseline, organizational structure configuration
  - Month 5: Public portal build (Experience Cloud), user registration/authentication, application forms
  - Month 6: Agency dashboards (Public Sector Solutions), workflow automation, master permit registry
  - Month 7: Mobile inspection app, automated refund system, fast-track processing, payment gateway integration
  - **Deliverable:** Functional sandbox environment with core capabilities
- **Phase 3: Integration Development (Months 8-10 | Jul - Sep 2026)**
  - Month 8: Agency system integrations (Commerce, Environmental Protection, Revenue), SSO implementation
  - Month 9: Additional integrations (Tourism, Transportation, Secretary of State), financial system connectivity
  - Month 10: Supporting service integrations (GIS, document storage, notification gateways), data migration execution

  - **Deliverable:** Integrated test environment with all system connections operational

- **Phase 4: Testing & Training (Months 10-12 | Sep - Nov 2026)**
  - Month 10: Unit and integration testing (concurrent with Phase 3)
  - Month 11: User acceptance testing with agencies, performance/security testing, FedRAMP validation, train-the-trainer program
  - Month 12: Final UAT, training delivery to agency staff, production readiness validation, go-live preparation
  - **Deliverable:** Production-ready system, trained users, go-live readiness certification
- **Phase 5: Go-Live (Month 13 | Jan 2027)**
  - Week 1-2 (Jan 1-15): Production deployment, cutover activities, system activation
  - Week 3-4 (Jan 16-31): Hypercare support (24/7), issue resolution, performance monitoring
  - **Deliverable:** Operational One-Stop-Shop Permitting Portal meeting statutory deadline

Post-Implementation Transition (Jan - Jun 2027)

- **January 1 - July 1, 2027:** Optional use period (dashboard available, paper applications still accepted)
- **July 1, 2027:** Mandatory use begins (dashboard becomes exclusive method)
- Continuous monitoring, user feedback collection, enhancement implementation, adoption support

Risk Mitigation and Schedule Assurance:

- **15% schedule buffer:** Built into critical path activities accommodating unforeseen delays
- **Parallel workstreams:** Configuration, integration, and training proceed simultaneously reducing overall timeline
- **Weekly executive steering:** Early identification and resolution of issues before they impact schedule
- **Hybrid Agile methodology:** Iterative development with continuous testing preventing late-stage surprises
- **Phased rollout option:** If needed, launch with core agencies first, add remaining agencies by July 2027
- **Pre-positioned resources:** IBM team ready to start immediately upon contract award
- **Critical Success Factors:**
- **Contract award by December 2025:** Any delay compresses implementation timeline
- **Agency participation:** Timely engagement from all seven departments in discovery and testing
- **Decision velocity:** Rapid resolution of design decisions and change requests
- **Data readiness:** Agencies prepare legacy data for migration during discovery phase
- **State IT support:** Timely provisioning of SSO access, network connectivity, and infrastructure support
- **Scope discipline:** Strict change control preventing scope creep that extends timeline

IBM's hybrid integration/replacement strategy preserves valuable agency investments while modernizing outdated systems, and our proven 13-month implementation timeline with phased delivery, parallel workstreams, and built-in buffers enables West Virginia meets the January 1, 2027 statutory deadline with confidence while minimizing risk and disruption.

4.2.1.16 Vendors should describe their approach on how to implement a "train-the-trainer" model, the vendor should deliver a structured, scalable training program that equips key agency users with the knowledge, tools, and confidence to train others effectively.

IBM implements a structured train-the-trainer model empowering key agency users to become system experts and effective trainers for their colleagues. This approach builds sustainable internal capability, reduces vendor dependency, and enables knowledge transfer remains within West Virginia state government. IBM partners with the State to identify, train, and certify agency champions who become first-line support and ongoing training resources for their departments.

Champion Selection:

IBM collaborates with agency leadership to identify ideal candidates:

- **Selection criteria:** 2-3 champions per agency with strong communication skills, technical aptitude, peer respect, and management support for 20% time dedication
- **Role diversity:** Mix of technical staff (system configuration) and business users (operational workflows)
- **Management commitment:** Written endorsement ensuring protected time for training responsibilities
- **Kickoff workshop:** Initial session setting expectations, roles, responsibilities, and success metrics

Intensive Champion Training (5 Days):

- **Days 1-2:** System Mastery
  - **Public portal:** Citizen/business user experience—application submission, document upload, payment, status tracking, renewals
  - **Agency back-office:** Public Sector Solutions queue management, application review, document annotation, approvals, collaboration
  - **Mobile inspection app:** Field capabilities including offline mode, checklists, photo capture, signatures, synchronization
  - **Advanced features:** Dashboard creation, report building, workflow modification using low-code tools
  - **Hands-on practice:** Guided exercises in training sandbox with realistic permit scenarios
  - **Troubleshooting: Common** issue identification and resolution
- **Day 3**: Administrative and Support Skills
  - **User management:** Account creation, password resets, permission assignment, role configuration
  - **Configuration basics:** Form modification, workflow adjustments, notifications using declarative tools
  - **Reporting and analytics:** Report generation, dashboard customization, data export
  - **Support processes:** Ticket logging, escalation, knowledge base article creation
  - **Security and compliance:** RBAC concepts, audit trails, data privacy
- **Day 4:** Training Skills and Adult Learning
  - **Adult learning principles:** How adults learn technology, accommodating different learning styles
  - **Presentation skills:** Engaging delivery, managing questions, handling difficult participants
  - **Demonstration best practices:** Screen sharing, pacing, cursor highlighting

  - **Hands-on facilitation:** Lab management, providing guidance without doing work for learners
  - **Assessment techniques:** Checking understanding, identifying struggling learners, providing support
  - **Feedback collection:** Surveys, observation, one-on-one check-ins
- **Day 5:** Practice and Certification
  - **Teach-back sessions:** Champions deliver 15-minute training segments with IBM observation and feedback
  - **Training material review:** Familiarization with all guides, reference cards, videos, FAQs
  - **Scenario role-play:** Handling questions, troubleshooting, escalating complex problems
  - **Knowledge assessment:** Written or practical exam validating proficiency
  - **Certification:** IBM issues Train-the-Trainer certificates
  - **Ongoing support plan:** Regular check-ins, monthly meetings, refresher sessions

Training Materials and Resources:

IBM develops comprehensive materials supporting champions and end users:

- **User Documentation:**
  - **Role-based user guides:** Separate manuals for public users, reviewers, inspectors, supervisors, administrators
  - **Quick reference cards:** Laminated one-page guides for common tasks
  - **Process flowcharts:** Visual step-by-step workflows for each permit type
  - **FAQ library:** Searchable repository with answers
  - **Glossary:** System-specific terms and definitions
- **Interactive Learning:**
  - **Video tutorials:** 5-10 minute task demonstrations with narration and captions
  - **Simulation environment:** Practice sandbox with sample data for risk-free exploration
  - **Interactive walkthroughs:** Click-through demonstrations with contextual help
  - **Scenario exercises:** Realistic case studies requiring end-to-end completion
  - **Knowledge checks:** Quizzes validating understanding after each module
  - **Training Presentation Materials:**
    - **PowerPoint decks:** Customizable presentations with speaker notes
    - **Demonstration scripts:** Step-by-step instructions for live system demos
    - **Lab guides:** Exercise instructions with expected outcomes
    - **Trainer tips:** Best practices, common mistakes, troubleshooting guidance
  - **Administrative tools**: Attendance rosters, feedback forms
- **Salesforce Trailhead:**
  - **Custom learning paths:** West Virginia-specific Trailhead modules
  - **Gamification:** Badges, points, leaderboards motivating self-paced learning
  - **Progress tracking:** Monitor completion rates and identify users needing support
  - **Continuous learning:** Ongoing content for new features

End-User Training Delivery:

Champions train colleagues using IBM-provided materials:

- **Role-based sessions:** Separate curricula by user type (2-4 hours per role)

- **Small cohorts:** 10-15 learners per session enabling personalized attention
- **Blended learning:** Instructor-led sessions, hands-on labs, self-paced online modules
- **Just-in-time scheduling:** Training 1-2 weeks before go-live maximizing retention
- **Multiple offerings:** Various dates/times accommodating schedules

Change Management Integration:

Training coordinated with broader adoption activities:

- **Pre-training communications:** Email campaigns explaining purpose, schedules, expectations
- **Executive messaging:** Leadership reinforcement of training importance
- **Success stories:** Highlighting early adopters building enthusiasm
- **Participation tracking:** Monitor attendance, identify non-participants
- **Go-live support:** Champions provide in-person assistance during first weeks
- **Post-training check-ins:** Address specific user questions
- **Performance support:** Job aids, cheat sheets at workstations
- **Recognition programs:** Acknowledge proficient users, high-performing agencies

Success Metrics:

Track key indicators validating training effectiveness:

- **Participation rates:** Percentage completing required training before go-live
- **Knowledge assessment scores:** Pre- and post-training tests demonstrating learning gains
- **User confidence ratings:** Self-reported comfort levels with system
- **System adoption rates:** Active logins, task completion volumes, feature utilization
- **Support ticket trends:** Declining basic questions indicating successful training
- **User satisfaction scores:** Overall training quality and effectiveness
- **Champion feedback:** Regular input on training experience and improvements
- Long-Term Sustainability:

Train-the-trainer model enables ongoing capability:

- **Internal expertise:** State owns training content, processes, delivery capability
- **Scalable model:** Champions train new hires, support additional agencies
- **Reduced costs:** Eliminate ongoing vendor training fees
- **Customization flexibility:** State modifies materials reflecting policy changes
- **Knowledge retention:** Training expertise remains within government
- **Continuous improvement:** Champions evolve training based on operational experience

IBM's train-the-trainer model builds sustainable internal training capability, empowers agency champions to effectively educate colleagues, reduces long-term vendor dependency, enables consistent high-quality training delivery across all agencies, and provides the State with tools, knowledge, and confidence to support the One-Stop-Shop Permitting Program independently, maximizing ROI and ensuring long-term success.

4.2.1.17 Vendors should describe how the solution provides a comprehensive, accessible, and self-paced learning platform like on-demand that supports both agency users and constituents after implementation.

As mentioned in 4.2.1.16, IBM's proposed solution leverages **Salesforce Experience Cloud** and **Salesforce Trailhead**, **Salesforce's widely used digital learning platform**, to deliver accessible, modular content. Trailhead provides interactive, scenario-based lessons, quizzes, and certifications that users can complete at their own pace. IBM can tailor these modules to

reflect the Agency's workflows, permitting processes, and data-security practices, making the platform highly relevant and easy to navigate.

For constituents, IBM will configure embedded help and learning resources within the public portal, including **tooltips, pop-up guidance, and short tutorial videos** that explain how to submit applications, upload documents, manage renewals, or track statuses. These features enable that external users receive guidance without needing formal classroom instruction.

4.2.1.18 The State currently uses Google and Microsoft products for core functions like email, calendar, and meetings, vendors should ensure their solution is compatible and interoperable with these platforms to streamline adoption and maximize productivity.

Salesforce seamlessly integrates with productivity tools widely used by state agencies including Google Workspace (Gmail, Calendar, Meet) and Microsoft 365 (Outlook, Exchange, Teams, OneDrive, SharePoint). IBM's integration expertise combined with MuleSoft Anypoint Platform enables full interoperability, allowing staff to work within familiar environments while leveraging the permitting platform.

Email and Calendar Integration:

- **Outlook/Exchange integration:** Sync emails, calendar appointments, contacts bidirectionally between Salesforce and Outlook
- **Gmail integration:** Similar synchronization capabilities for Google Workspace users
- **Email-to-case:** Automatically create application support tickets from inbound emails
- **Activity logging:** Emails and meetings related to permit applications automatically attached to records
- **Inspection scheduling:** Calendar integration displaying inspection appointments in staff Outlook/Google Calendar
- **Meeting invitations:** Generate calendar invites directly from Salesforce for applicant meetings, site visits, hearings

Collaboration Platform Integration:

- **Microsoft Teams:** Embed Salesforce records in Teams channels; receive notifications; collaborate on permit reviews without leaving Teams
- **Google Meet:** Launch video meetings directly from Salesforce application records
- **Shared channels:** Create Teams/Slack channels linked to specific permit applications for multi-agency coordination
- **Document collaboration:** Edit Word/Excel documents stored in Salesforce using Office 365 online editors

Document Storage Integration:

- **OneDrive/SharePoint:** Store and access permit documents in agency SharePoint libraries while managing metadata in Salesforce
- **Google Drive:** Similar integration for agencies using Google Workspace
- **Version control:** Maintain document versions across both systems
- **Permission sync:** Salesforce RBAC enforced when accessing documents in SharePoint/Drive

Benefits:

- **Streamlined adoption:** Staff continue using familiar email, calendar, collaboration tools reducing training burden
- **Increased productivity:** No context switching between applications; work seamlessly across platforms

- **Unified communication:** All permit-related correspondence centralized in Salesforce regardless of originating tool
- **Reduced duplication:** Automatic activity logging eliminates manual data entry

Integration with existing productivity tools enables staff to leverage the permitting platform without abandoning familiar workflows, accelerating adoption and maximizing efficiency.

4.2.1.19 Vendors should explain how the solution can be adjusted to meet the growing and changing needs of the State. The State anticipates additional agencies may desire to participate in the solution in the future, the platform should be able to evolve alongside the State's operational, technical, and organizational growth, flexible and scalable to adapt to increased requirements in future years.

IBM's solution is built on Salesforce's cloud-native architecture designed for unlimited scalability and rapid adaptation. The platform's low-code configuration approach enables the State to add agencies, create new permit types, modify workflows, and scale transaction volumes without platform replacement or redevelopment. As West Virginia's permitting needs evolve, the solution grows seamlessly through declarative configuration and elastic cloud infrastructure.

Adding New Agencies:

Structured process accommodates additional agencies with minimal disruption:

- **Templated deployment:** pre-configured organizational structure, roles, permissions, workflows replicated and customized for new agencies in 4-6 weeks
- **Incremental implementation:** Agencies added individually without impacting existing operations
- **Pilot programs:** Start with subset of permit types, expand gradually based on readiness
- **Pay-as-you-grow:** User licenses purchased as agencies join; no large upfront investment

Scalability for Volume Growth:

Cloud-native architecture automatically scales with increasing demand:

- **Elastic infrastructure:** Automatic resource provisioning as transaction volumes increase
- **Unlimited storage:** No artificial limits on permits, applications, documents, or historical records
- **Performance maintained:** Sub-second response times regardless of user base or data volume growth
- **Concurrent users:** Handles thousands of simultaneous public users and agency staff without degradation

Adding and Modifying Permit Types:

Low-code tools enable rapid changes without vendor involvement:

- **Form builder:** State administrators create new permit forms using OmniStudio drag-and-drop interface in days
- **Workflow configuration:** Define approval routing, review stages, escalations using Salesforce Flow visual tools
- **Template reuse:** Clone similar existing permits as starting point, modify as needed
- **Business rule updates:** Modify validation rules, conditional logic, notifications without programming
- **Fee schedule changes:** Configure fees, calculations, fast-track premiums responding to policy changes

Regulatory and Legislative Response:

Rapid adaptation to new statutory or policy requirements:

- **Emergency procedures:** Fast-track process for critical updates meeting urgent legislative mandates
- **Deadline modifications:** Quickly implement new processing timelines, refund rules, approval criteria
- **Compliance reporting:** Add new reports, analytics, data exports as regulations evolve

Technology Evolution:

Platform continuously improves through Salesforce innovation:

- **Three annual releases:** Spring, Summer, Winter releases with new features, security patches, performance improvements automatically available at no additional cost
- **AI enhancements:** AI capabilities continuously improved—better chatbots, smarter predictions, advanced analytics
- **Security updates:** Continuous vulnerability patches, compliance certifications
- **Mobile improvements:** Native apps updated with new features, UI enhancements, OS compatibility

Self-Service Administration:

State staff empowered to manage ongoing changes independently:

- **Delegated administration:** Agency administrators manage users, permissions, configurations without IT intervention
- **Low-code tools:** Point-and-click configuration accessible to business users without programming skills
- **Sandbox testing:** Test changes in non-production environments before deploying live
- **Comprehensive documentation:** Guides, videos, knowledge base enabling self-sufficiency
- **Reduced vendor dependency:** State increasingly manages enhancements, new permits, agency additions independently

Integration Extensibility:

Flexible architecture accommodates new system connections:

- **API-first design:** RESTful APIs expose all functionality for future integrations
- **Modular integration:** Add connections to new systems without impacting existing integrations
- **Standard protocols:** SAML, OAuth, SOAP, REST ensuring compatibility with emerging technologies

Capacity Planning:

Proactive management ensuring platform grows ahead of demand:

- **Usage analytics:** Track transaction volumes, storage, user growth identifying capacity needs
- **Quarterly reviews:** Regular capacity planning sessions ensuring alignment with State IT
- **Transparent forecasting:** TCO projections accounting for growth scenarios
- **Proactive scaling:** Increase resources before constraints arise

IBM's solution provides West Virginia with a future-proof platform that scales seamlessly as agencies join, volumes grow, and requirements evolve. Cloud-native elasticity, low-code configurability, and continuous Salesforce innovation enable the One-Stop-Shop Permitting

Program adapts dynamically to the State's growth trajectory without costly replacements, maximizing ROI and ensuring long-term sustainability.

4.2.1.20 Vendors should demonstrate commitment to high system availability, transparent maintenance practices, and rapid recovery protocols with downtime and planned maintenance windows being outside of business hours.

IBM's solution enables high system availability, transparent maintenance practices, and rapid recovery protocols with all planned downtime scheduled outside business hours. The solution leverages Salesforce Government Cloud's enterprise-grade reliability with proactive monitoring, automated failover, and documented disaster recovery procedures minimizing disruption to State operations.

High System Availability:

IBM maintains enterprise-level reliability through comprehensive monitoring and redundancy:

- **Proactive monitoring:** 24/7 system health monitoring with automated alerting identifying potential issues before impact
- **Multi-region redundancy:** Automatic failover between US East and US West data centers in under 5 minutes
- **FedRAMP High infrastructure:** Salesforce Government Cloud availability consistent with federal standards
- **Capacity planning:** Regular analysis with proactive scaling preventing performance degradation
- **Load balancing:** Automatic workload distribution across servers preventing bottlenecks
- **99.9% uptime SLA:** Enterprise service level agreement with financial penalties for non-compliance

Transparent Maintenance Practices:

IBM operates with full transparency throughout operations and maintenance:

- **Advance notification:** 14 days notice for major changes, 7 days for minor updates via email, portal announcements, status page
- **Maintenance calendar:** Published monthly schedule showing all planned activities
- **Change documentation:** All maintenance procedures documented in Integrated Project Management Plan and tracked in IBM PMIS
- **Performance dashboards:** Real-time visibility into system health, capacity utilization, incident metrics shared with State stakeholders
- **Regular reporting:** Monthly maintenance reports detailing activities performed, issues resolved, performance trends
- **Stakeholder communication:** Dedicated communication channels for real-time updates during maintenance windows

Rapid Recovery Protocols:

Tested disaster recovery and business continuity procedures enable rapid restoration:

- **Disaster Recovery Plan:** Documented procedures tested quarterly through tabletop exercises and failover drills
- **Recovery objectives:** RTO 4 hours, RPO 4 hours, maximum tolerable downtime 8 hours
- **Real-time replication:** Continuous data synchronization to secondary data center
- **Automated backups:** Incremental backups every 4 hours, full daily backups, 90-day retention
- **Incident escalation:** Defined escalation paths with 15-minute response for critical incidents

- **Business continuity:** Multi-region deployment ensuring operations continue during site-level failures
- **Validation testing:** Annual comprehensive DR tests with documented results and improvement actions

Maintenance Scheduling:

All planned maintenance scheduled outside business hours minimizing operational disruption:

- **Maintenance windows:** Saturday 10 PM - Sunday 6 AM Eastern Time
- **Advance coordination:** Schedule confirmed with State leadership 14+ days prior
- **Emergency maintenance:** Pre-approved protocols for critical security patches with minimum 2-hour notification
- **Impact assessment:** All changes evaluated for risk; low-impact changes bundled to reduce frequency
- **Rollback procedures:** Tested rollback plans if maintenance causes unexpected issues
- **Extended hours support:** Technical team available during maintenance windows for immediate issue resolution
- **Public communication:** Status page updates and portal notifications informing users of scheduled maintenance

Incident Response:

Structured protocols for unplanned outages:

- **Immediate response:** Incident team activates within 15 minutes of detection
- **Status communications:** Updates every 30 minutes via status page, email, SMS until resolution
- **Root cause analysis:** Post-incident review within 5 business days identifying cause and preventive measures
- **Corrective actions:** Implementation of improvements preventing recurrence
- **Transparent reporting:** Incident reports shared with State leadership documenting timeline, impact, resolution

Performance Monitoring:

Continuous tracking ensuring optimal system performance:

- **Real-time metrics:** Response times, transaction volumes, error rates, resource utilization
- **Proactive alerting:** Automated notifications when thresholds exceeded enabling preemptive action
- **Trend analysis:** Identification of performance degradation patterns before user impact
- **Optimization recommendations:** Regular suggestions for configuration improvements enhancing performance
- **Monthly performance reviews:** Stakeholder meetings reviewing metrics, identifying optimization opportunities

Customer Support and Contact Center

IBM can provide customer support and contact center services to assist citizens and agency users with portal inquiries, password resets, and application guidance. These services can be delivered through IBM's U.S. based support centers and integrated with the permitting platform's case management module. Final scope, staffing levels, and service hours coverage will be defined and agreed upon during the Discovery Phase, once the State's volume and operational requirements are confirmed.

IBM's commitment to high availability, transparent maintenance, and rapid recovery enables the One-Stop-Shop Permitting Program maintains 99.9% uptime with all planned maintenance outside business hours, proactive monitoring preventing issues before impact, documented disaster recovery procedures tested quarterly, and transparent communication keeping stakeholders informed—delivering reliable, uninterrupted service to West Virginia citizens, businesses, and agency staff.

4.2.1.21 Vendors' solution must include a description of the project management approach and relevant tools to be utilized.

IBM will manage this engagement using its proven, global delivery framework known as the Worldwide Project Management Methodology (WWPMM)—a structured, experience-based approach aligned with the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK®) standards.

This methodology provides the governance, processes, and tools required to plan, execute, monitor, and control all phases of the project—from kickoff through implementation, transition to operations, and project closeout. WWPMM has been refined over decades of large-scale technology and systems modernization programs across public-sector clients and is tailored to enable transparency, quality, and measurable business outcomes.

Core Tenets of IBM's Project Management Methodology

IBM's project management framework is built upon four guiding principles:

1. Defined Processes and Planning Discipline

IBM conducts a structured Definition and Planning Phase to enable that project scope, schedule, risk factors, deliverables, and governance structures are clearly understood and agreed upon by all stakeholders.

Key processes include:

- Communication management
- Quality and risk management
- Change control and configuration management
- Resource and budget planning
- Status reporting and issue escalation procedures

2. Project Organization and Responsibilities

IBM collaborates with the Agency to define the project governance structure, including project sponsors, steering committee members, IBM leads, and state participants.

Roles and responsibilities are documented in a RACI matrix and the Integrated Project Management Plan (IPMP), ensuring accountability and clarity across both IBM and Agency teams.

3. Phased Project Lifecycle with Clear Milestones

The work is organized into phases such as:

- Initiation and Planning
- Requirements, Discovery, and Design
- Configuration and Development
- Quality Assurance and Testing
- Deployment and Hypercare
- Maintenance and Operations (M&O)

Each phase includes defined entry and exit criteria and formal Phase Gate Reviews (PGRs) to validate quality, completeness, and readiness to proceed.

4. Project Management System and Tool Integration

IBM uses a customized Project Management Information System (PMIS) that provides real-time visibility into progress, risks, costs, and deliverables. This system integrates with IBM's collaboration and reporting tools to enable consistent governance across the project.

Tools Utilized in the Engagement

IBM employs a combination of enterprise-grade and collaborative tools to enable efficient management, communication, and transparency. These include:

Tool / Platform	Purpose and Use in Engagement
IBM Project Management Information System (PMIS)	Centralized repository for schedules, deliverables, risks, issues, and status tracking. Provides dashboards for project health and performance indicators.
Microsoft Project / Smartsheet	Used to build and maintain the master schedule, WBS, milestones, and dependencies. Supports critical path and resource tracking.
Jira / Azure DevOps	For sprint planning, backlog management, and issue tracking; integrates with testing tools to support continuous delivery.
IBM Blueworks Live	Business process mapping tool used during discovery to visualize current and future workflows.
IBM Quality Manager / Rational Team Concert	For quality assurance, configuration management, and version control of deliverables and documentation.
IBM Box / SharePoint / Teams	Secure collaboration, document management, and communication between IBM and Agency stakeholders.
IBM Cognos Analytics or Salesforce CRM Analytics	Used for executive dashboards and reporting on project KPIs, resource utilization, and milestone performance.
IBM Security and Compliance Tools	Support auditability and compliance with state and federal security requirements throughout delivery.

All tools are configured to comply with the Agency's cybersecurity policies and hosted within IBM's or Salesforce's secure cloud environments.

4.2.1.22 Vendor should be able to integrate with the State's Single Sign-On Solution.

Salesforce supports single sign-on (SSO) to allow users to log in once and access multiple connected applications. This includes industry-standard authentication protocols such as SAML 2.0, OpenID Connect, and OAuth 2.0.

These standards allow Salesforce to integrate directly with government and enterprise identity providers (IdPs) such as Microsoft Azure Active Directory, Okta, Ping Federate, Google Workspace, and other state-operated identity management systems.

4.2.1.23 Vendor's pricing page should provide a total and complete implementation and build out cost, and should identify any milestone payment expectations. Vendor's pricing page should also provide proposed annual licensing costs, hosting costs, maintenance costs, and other cost breakdowns.

IBM's pricing is provided as a separate document. Please see IBM's Cost Proposal for information.

4.2.1.24 Vendor should guarantee that all work on this project will be performed in the United States. Use of technology to communicate with countries banned by the Federal Government is prohibited.

IBM acknowledges that **all work on this project will be performed entirely within the United States**. No project activities, data processing, or support functions will be conducted or transferred outside U.S. territory. IBM further affirms that the company will **not use or permit the use of any technology, communication, or collaboration tools that connect to, route through, or engage with countries banned or restricted by the Federal Government**. All personnel assigned to the project and all supporting systems will comply fully with applicable federal, state, and agency security and export-control requirements.

4.2.1.25 Vendor should provide constituents access to a digital wallet for payment, refund, and license/permit management.

IBM confirms our solution fully satisfies this requirement through an integrated digital wallet capability built on Salesforce's native payment processing framework. The wallet serves as a centralized hub enabling West Virginia constituents to manage payment methods, track transactions, store digital permits, and receive automated refunds—all within a secure, PCI-DSS compliant environment accessible from any device.

Payment Method Management

Supported Payment Types:

- Major credit/debit cards (Visa, Mastercard, Amex, Discover)
- ACH/eCheck direct bank payments
- Digital wallets (Apple Pay, Google Pay, PayPal)

Security & Convenience:

- **PCI-DSS Level 1 compliance** with tokenization—card numbers never stored in Salesforce
- **FIPS 140-3 encryption** protects all payment credentials
- **Multi-Factor Authentication (MFA)** required for adding/modifying payment methods
- **One-click payments** after initial setup with ability to manage multiple methods
- **Default payment designation** with option to select alternatives at checkout
- **Automatic expiration alerts** at 60 days with prompts to update
- **Fraud detection** monitors suspicious activity patterns

Transaction Processing & History

Real-Time Payment Features:

- Instant authorization with immediate confirmation to applicant and agency
- Split payments across multiple methods for large fees
- Payment plans for high-value permits (installments)
- Automatic renewal charges (opt-in) for expiring permits
- Transparent fee display including processing charges and fast-track premiums
- Immediate receipt generation (printable/downloadable PDF)
- Automatic retry logic with alternate methods if primary payment fails

Complete Transaction Tracking:

- Comprehensive history of all payments, refunds, and adjustments with date/time stamps
- Filter/search by date range, permit type, or amount
- Export to PDF/CSV for accounting purposes

- Year-end summaries for tax preparation
- Running balance across all permits
- Indefinite retention of financial records

Automated Refund Processing

Statutory Compliance (§5A-13-4):

When agencies miss processing deadlines, the system automatically:

1. Flags application for mandatory refund within minutes of deadline expiration
2. Calculates total refund (application fees + fast-track premiums + processing charges)
3. Initiates refund through payment gateway without applicant action
4. Routes refund to original payment method

Refund Methods:

- **Primary:** Original payment method (cards: 3-5 days; ACH: 5-7 days)
- **Secondary:** Alternative stored method if original expired/closed
- **Tertiary:** State warrant (check) if no valid electronic method
- **Optional:** Digital wallet credit for future applications

Refund Transparency:

- Immediate email/SMS notification explaining reason and timeline
- Real-time status tracking: Pending → Processing → Completed
- Confirmation when refund posts
- Complete refund history linked to associated applications
- Automatic handling of partial refunds for split/installment payments

Digital License & Permit Storage

Centralized Credential Repository:

- All active permits, licenses, certificates stored in one secure location
- Full details: issuance date, expiration, permit number, agency, conditions
- **QR codes** for instant verification by inspectors and enforcement
- Official PDF downloads with state seal for printing
- Apple Wallet/Google Pay integration for offline mobile access

Organization & Management:

- Categorization by type (business, environmental, construction, professional)
- Color-coded status indicators: Active / Expiring Soon / Expired / Suspended
- Quick filters by type, agency, or status
- Pin frequently-accessed permits to top
- Secure 24-hour temporary links to share with contractors/partners

Proactive Expiration Management:

- Visual countdown showing days until expiration
- Automatic reminders at 90, 60, 30 days via email/SMS/dashboard
- One-click renewal with pre-populated data
- Optional auto-renew with stored payment method (if eligible)
- Grace period tracking for expired-but-renewable permits

Verification & Compliance:

- Inspector portal validates permits via QR scan in real-time
- Audit trail of all views, shares, and verifications
- Automatic alerts for suspensions, revocations, or condition changes
- Linked storage for supporting documents (insurance, site plans, inspections)

Mobile Accessibility

Responsive Design:

- Adaptive interface optimized for smartphones, tablets, desktops
- Touch-optimized controls and swipeable card layouts
- Device camera integration for credit card scanning
- Biometric authentication (Face ID, Touch ID, fingerprint)

Native Mobile Features:

- Salesforce Mobile App for iOS/Android
- Push notifications for payments, refunds, expiring permits
- Offline access to stored permits and transaction history
- GPS-aware features for location-based permit display

Accessibility & Compliance

Universal Access:

- **WCAG 2.2 AA compliant** with screen reader support
- Keyboard navigation for all wallet functions
- High-contrast mode and adjustable text sizing
- Bilingual interface (English/Spanish)
- Plain language descriptions (8th-grade reading level)

Assistive Options:

- Telephone support for vision-impaired users to check balances and transactions
- Large-print transaction statements available on request
- In-person assistance at agency offices for digital wallet setup

Technical Implementation

Platform Foundation:

- Built on Salesforce Experience Cloud with native payment processing APIs
- Integrated with state-approved payment gateway (selection during procurement)
- Real-time synchronization with agency back-office financial systems
- State accounting/ERP integration for revenue tracking and reconciliation

Security Architecture:

- End-to-end TLS 1.3 encryption for all transactions
- Tokenization via PCI-certified vault—no raw card data in Salesforce
- Role-Based Access Control with session timeouts (15 min public users)
- 24/7 fraud monitoring with automated suspicious activity blocking
- Complete audit logging retained 7 years per state records policy

Data Protection:

- All wallet data encrypted at rest using AES-256 (FIPS 140-3)

- Hosted in FedRAMP High authorized Salesforce Government Cloud
- US-only data residency with no offshore processing
- Annual PCI-DSS validation and penetration testing

User Experience Benefits

For Citizens & Businesses:

- **Eliminate redundant data entry** with stored payment methods and permit information
- **24/7 self-service access** to financial records and credentials from any device
- **Instant refunds** without filing claims or contacting agencies
- **Paperless convenience** with digital permits replacing physical documents
- **Proactive notifications** prevent lapses and missed renewal deadlines
- **Consolidated view** of all state permits and licenses across agencies

For Agencies:

- **Automated refund compliance** eliminates manual processing and budget errors
- **Reduced call volume** as constituents self-serve payment and permit inquiries
- **Real-time revenue visibility** with automatic accounting system integration
- **Instant permit verification** by field inspectors via QR scanning
- **Audit trail completeness** for financial compliance and legislative oversight

For State Leadership:

- **Economic development enablement** through faster, easier business transactions
- **Transparency demonstration** showing real-time refund accountability
- **Cost savings** reducing paper, postage, and manual processing
- **Constituent satisfaction** improvement through modern digital services
- **Data-driven insights** on payment patterns, renewal rates, and refund trends

Scalability & Future Enhancement

The digital wallet architecture is designed for continuous evolution:

- Additional payment methods easily integrated (cryptocurrencies, installment financing)
- Wallet-to-wallet transfers for permit ownership changes
- Subscription models for recurring permits with automatic renewals
- Loyalty programs offering fee discounts for early renewals or online-only applications
- Third-party integrations with business accounting software (QuickBooks, Xero)
- Blockchain audit trails for immutable permit history (future enhancement)

IBM's digital wallet solution transforms West Virginia's permitting process into a modern, constituent-centric experience while ensuring full compliance with statutory refund requirements, providing secure credential management, and positioning the State as a leader in digital government services.

4.2.2. Mandatory Project Requirements

The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor shall describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

4.2.2.1 Vendors must provide a solution for the development and creation of a one-stop shop permitting portal.

IBM confirms that it meets this mandatory requirement.

IBM will provide a comprehensive solution for the development and creation of a one-stop shop permitting portal as specified in the RFP. Our proposed solution delivers a unified, digital platform consolidating all permit and license types from participating state agencies into a single interface accessible to citizens, businesses, and agency staff.

The solution includes:

- **Public-facing portal:** Experience Cloud-based interface enabling citizens and businesses to apply for permits, upload documents, pay fees, track application status, and manage licenses from any device
- **Internal agency dashboards:** Public Sector workspaces providing staff with tools for application review, workflow management, inspection coordination, and performance monitoring
- **Integrated functionality:** Complete end-to-end permitting lifecycle from application submission through review, inspection, approval, issuance, and renewal
- **Multi-agency consolidation:** Single platform supporting all seven participating departments (Commerce, Environmental Protection, Environmental Health Services, Tourism, Secretary of State, Revenue, Transportation)
- **Statutory compliance:** Automated deadline tracking, refund triggering, fast-track processing, and all capabilities required under West Virginia Code §5A-13-1 et seq.

IBM's solution fully satisfies the mandatory requirement to develop and create a one-stop shop permitting portal, delivering the comprehensive digital transformation envisioned by House Bill 2002 and meeting the January 1, 2027 statutory implementation deadline.

4.2.2.2 Vendors' solution must outline a structured, transparent, and collaborative methodology that ensures timely delivery, stakeholder alignment, and quality assurance throughout the implementation lifecycle.

IBM confirms that it meets this mandatory requirement.

IBM's solution outlines a structured, transparent, and collaborative methodology ensuring timely delivery, stakeholder alignment, and quality assurance throughout the implementation lifecycle. Our approach combines IBM's Worldwide Project Management Methodology (WWPMM)—aligned with PMI's PMBOK® standards—with Hybrid Agile delivery practices and Enterprise Design Thinking, providing disciplined governance while maintaining flexibility to adapt as requirements evolve.

Structured Project Governance:

IBM's methodology provides repeatable framework managing all project dimensions:

- **Defined project phases:** Planning, design, configuration, testing, deployment, maintenance with documented deliverables and phase-gate reviews
- **WWPMM framework:** Manages scope, schedule, cost, risk, and quality with measurable progress tracking
- **Milestone-based delivery:** Clear checkpoints with approval gates ensuring work meets standards before advancing
- **Dependency management:** Tracking and coordination of interdependencies preventing delays
- **Predictable delivery cadence:** Iterative development cycles producing measurable outcomes on time and within budget

Transparency and Accountability:

Real-time visibility into project status for all stakeholders:

- **Integrated Project Management Plan (IPMP):** Single source of truth for project activities, dependencies, and deliverables
- **Project Management Information System (PMIS):** Centralized platform providing near real-time visibility into status, risks, issues
- **Regular governance meetings:** Executive steering committee, weekly status reports, risk tracking, decision logs
- **Performance dashboards:** Visual displays of progress against milestones, budget, and quality metrics
- **Quality and Delivery Excellence reviews:** Independent expert validation that work meets contractual and technical standards

Collaboration and Stakeholder Alignment:

Continuous engagement ensuring solution meets State needs:

- **Enterprise Design Thinking workshops:** Co-creation sessions with agency leadership, program managers, and end users
- **Sprint reviews:** Bi-weekly demonstrations of working functionality with stakeholder feedback
- **Playback sessions:** Validation of designs and prototypes before development reducing rework
- **User acceptance testing:** Representative users validate functionality before deployment
- **Change management integration:** Training, communication, and adoption activities aligned with technical delivery

Quality Assurance:

Quality embedded throughout project lifecycle, not just at end:

- **Acceptance criteria:** Predefined standards for each deliverable with formal review processes
- **Phase gate reviews:** Independent validation of readiness before advancing to next stage
- **Sprint retrospectives:** Continuous improvement capturing lessons learned during implementation
- **Multi-level testing:** Unit, integration, performance, security, accessibility, and user acceptance testing
- **Post-deployment monitoring:** Ongoing performance tracking, health checks, and optimization

IBM's structured, transparent, and collaborative methodology enables the One-Stop-Shop Permitting Program is delivered on time (January 1, 2027 statutory deadline), within scope, aligned with stakeholder needs, and to the highest quality standards—providing West Virginia with confidence in successful implementation and long-term platform sustainability.

4.2.2.3 Vendor must agree to and meet all data security requirements identified by the Office of Technology, for the entirety of the project, including initial meetings, information gathering, development, and other preliminary stages.

IBM confirms that it meets this mandatory requirement.

IBM agrees to and will meet all data security requirements identified by the Office of Technology for the entirety of the project, including initial meetings, information gathering, development, and all preliminary stages through implementation, operations, and ongoing maintenance.

IBM's commitment includes:

- **Full compliance:** Adherence to all Office of Technology data security policies, standards, and requirements throughout all project phases
- **All project stages:** Security requirements enforced during discovery, design, development, testing, deployment, and operations
- **Comprehensive protection:** Safeguarding of all State data, personally identifiable information (PII), and sensitive information accessed, processed, or stored during the engagement
- **Continuous compliance:** Ongoing adherence to security requirements as they evolve or are updated by the Office of Technology
- **Documentation and reporting:** Regular security compliance reporting and evidence of adherence to Office of Technology requirements
- **Incident notification:** Immediate reporting of any security incidents or potential vulnerabilities to Office of Technology per established protocols

IBM will execute any required security agreements, complete all necessary security assessments, and participate in security reviews as directed by the Office of Technology. Our team will coordinate closely with Office of Technology staff to enable alignment with State cybersecurity policies and requirements throughout the entire engagement.

4.2.2.4 Vendor's proposed solution must meet FedRAMP requirements.

IBM confirms that it meets this mandatory requirement.

IBM's proposed solution meets all FedRAMP requirements. The solution is built on Salesforce Public Sector Solutions (PSS) and hosted within Salesforce Government Cloud Plus, which holds **FedRAMP High authorization**—the highest level of federal cloud security authorization.

IBM's FedRAMP compliance includes:

- **FedRAMP High authorization:** Salesforce Government Cloud Plus is authorized at FedRAMP High impact level, meeting stringent federal security requirements for systems processing sensitive data
- **NIST 800-53 Rev 5 controls:** Implementation of all required security controls across 20 control families including access control, audit and accountability, identification and authentication, incident response, and system protection
- **FIPS 140-3 encryption:** All data encrypted at rest using AES-256 and in transit using TLS 1.3 with FIPS-validated cryptographic modules
- **Continuous monitoring:** 24/7 security operations center (SOC) monitoring with automated threat detection and incident response

- **Annual assessments:** Regular third-party security assessments validating ongoing compliance with FedRAMP requirements
- **Data protection:** All constituent data, personally identifiable information (PII), and business data protected according to federal standards for confidentiality, integrity, and availability

IBM will configure, implement, and operate the system within this FedRAMP-authorized environment while aligning all project governance and controls with federal cybersecurity standards and State of West Virginia cybersecurity policies, ensuring continuous compliance throughout the engagement.

4.2.2.5 Vendor must ensure all state Data is encrypted at rest and during transit. Encryption must meet FIPS 140-3 standard.

IBM confirms that it meets this mandatory requirement.

IBM enables all State data is encrypted at rest and during transit using cryptographic modules validated to the FIPS 140-3 standard—the current Federal Information Processing Standard for cryptographic security.

IBM's encryption implementation includes:

- **Encryption at rest:** All data stored in Salesforce Government Cloud encrypted using AES-256 encryption with FIPS 140-3 validated cryptographic modules
- **Encryption in transit:** All data transmitted between users and the platform, and between integrated systems, encrypted using TLS 1.3 protocol with FIPS 140-3 validated cryptographic modules
- **Shield Platform Encryption:** Salesforce native field-level encryption protecting sensitive data including personally identifiable information (PII), Social Security numbers, payment data, and proprietary business information with automated key management and rotation
- **End-to-end protection:** Comprehensive encryption covering all data types including application data, documents, attachments, communications, and system metadata
- **Key management:** Secure cryptographic key generation, storage, rotation, and destruction following federal standards
- **Compliance validation:** Regular third-party assessments verifying FIPS 140-3 compliance and proper encryption implementation

This encryption strategy protects the confidentiality and integrity of all constituent, business, and administrative data handled by the One-Stop-Shop Permitting system while fully aligning with FedRAMP High and NIST SP 800-53 Rev 5 security controls, ensuring West Virginia's data remains secure throughout all project phases and ongoing operations.

4.2.2.6 Vendor is responsible for ensuring any subcontractors utilized in this project are identified and reported to the WV Office of Technology and that such subcontractors (if applicable) always maintain compliance with the State's data security requirements. The Contractor may not assign, transfer, or subcontract any portion of the contract without the State's prior written consent.

IBM confirms that it meets this mandatory requirement.

IBM intends to self-preform this work if awarded. IBM acknowledges full responsibility for ensuring any potential subcontractors utilized in this project are identified and reported to the West Virginia Office of Technology and that such subcontractors always maintain compliance with the State's data security requirements. IBM will not assign, transfer, or subcontract any portion of the contract without the State's prior written consent.

4.2.2.7 Vendor's security controls must be in accordance with the NIST 800-53 standard. Vendor must provide evidence of this upon request

IBM confirms that it meets this mandatory requirement.

IBM's security controls are designed and implemented in full accordance with NIST Special Publication 800-53 standard, which provides the foundational framework for federal information system security and aligns with FedRAMP High requirements. IBM will provide evidence of compliance upon request.

IBM's NIST 800-53 compliance includes:

- **Comprehensive control implementation:** All applicable NIST 800-53 Rev 5 security controls implemented across 20 control families including access control, audit and accountability, identification and authentication, incident response, system and communications protection, and configuration management
- **FedRAMP alignment:** Salesforce Government Cloud Plus FedRAMP High authorization validates NIST 800-53 compliance through rigorous third-party assessment
- **Control documentation:** Detailed security plans, policies, procedures, and control implementation statements documenting how each applicable NIST 800-53 control is satisfied
- **Assessment evidence:** Security assessment reports, test results, vulnerability scans, penetration tests, and continuous monitoring data demonstrating ongoing compliance
- **IBM governance integration:** IBM's Worldwide Project Management Methodology (WWPMM) integrates NIST 800-53 requirements into project governance, quality reviews, and delivery processes
- **Continuous compliance:** Ongoing monitoring, quarterly assessments, and annual security audits ensuring sustained adherence to NIST 800-53 requirements
- **Evidence availability:** Comprehensive documentation maintained and made available to the State and Office of Technology upon request including security plans, control matrices, assessment reports, and compliance certifications

IBM is committed to transparency and accountability—all security documentation, procedures, and quality review records will be maintained throughout the engagement and provided to the State upon request as evidence of compliance with NIST 800-53 and applicable federal standards.

4.2.2.8 Vendor must demonstrate how the solution implements a proactive, transparent, and standards-based security program that ensures system integrity and compliance with state cybersecurity expectations. Solution must provide security vulnerability scanning and routine reports of such testing of the system to the Office of Technology at routine intervals and upon request.

IBM confirms that it meets this mandatory requirement.

IBM's solution implements a proactive, transparent, and standards-based security program that continuously monitors for threats, conducts regular vulnerability scanning, and provides the Office of Technology with detailed routine and on-demand security reports. This approach enables ongoing compliance with state cybersecurity expectations, rapid remediation of issues, and sustained system integrity throughout the solution's lifecycle.

Proactive Security Framework:

IBM's security program is rooted in federal and industry standards ensuring comprehensive protection:

- **Standards alignment:** NIST 800-53 Rev 5, FIPS 140-3, FedRAMP High controls validated through Joint Authorization Board (JAB)
- **FedRAMP authorized environment:** Salesforce Government Cloud Plus provides continuous vulnerability scanning, configuration management, and audit logging
- **Role-Based Access Control:** RBAC with least privilege enforcement restricting access to authorized functions and data
- **Multi-Factor Authentication:** MFA required for all administrative and privileged accounts
- **FIPS 140-3 encryption:** Data encrypted at rest and in transit using validated cryptographic modules
- **Secure configuration baselines:** Patch management and configuration controls aligned with NIST SP 800-137 (Continuous Monitoring)
- **Defense in depth:** Multi-layered security across network, application, data, and identity levels

Vulnerability Scanning and Continuous Monitoring:

Automated scanning and real-time monitoring identifying threats before exploitation:

- **Automated vulnerability scanning:** FedRAMP-approved tools scanning application, infrastructure, and integrations
- **Routine scan schedule:** Weekly automated scans with additional scans following major updates or changes
- **Continuous monitoring:** 24/7 Security Operations Center (SOC) with real-time alerts for anomalous activity, unauthorized access attempts, or performance anomalies
- **Threat intelligence integration:** Proactive identification of emerging vulnerabilities and attack vectors
- **Remediation workflow:** Findings triaged by severity (critical, high, medium, low) with defined resolution timelines—critical vulnerabilities remediated within 72 hours
- **Verification testing:** Re-scanning confirms vulnerability closure before marking resolved
- **Independent quality reviews:** IBM Delivery Excellence team and Salesforce Security Operations Center validate vulnerability management compliance
- **Documentation:** All scanning activities, findings, and remediation tracked in IBM's Project Management Information System (PMIS)

Transparent Security Reporting:

Comprehensive reporting providing Office of Technology full visibility:

- **Routine reports:** Monthly security reports delivered to Office of Technology including vulnerability scan results, remediation status, security events, and compliance metrics
- **On-demand reporting:** Additional reports provided upon Office of Technology request at any time
- **Report contents:** Summary of vulnerability scans and results, remediation status and timelines for identified issues, security event and incident response summaries, configuration compliance metrics, patch management status, threat intelligence updates
- **Dashboard access:** Real-time security dashboards accessible to designated state cybersecurity personnel showing current security posture and compliance status
- **Audit logs:** Comprehensive audit trails available for Office of Technology review documenting all security-relevant activities
- **Trend analysis:** Historical trending identifying patterns and improvement opportunities
- **Executive summaries:** High-level security status reports for State leadership

Incident Response:

Structured protocols ensuring rapid response and transparent communication:

- **Incident Response Plan:** Documented procedures aligned with NIST 800-61 and state incident management requirements
- **Immediate notification:** Office of Technology notified within required timeframes for security incidents per state policy
- **24/7 availability:** Security team on-call for incident response
- **Escalation procedures:** Documented chain of command with defined escalation criteria and timelines
- **Containment and remediation:** Rapid actions limiting incident impact and restoring normal operations
- **Post-incident review:** Root cause analysis, lessons learned, and preventive measures implemented
- **Regular testing:** Incident response and business continuity plans tested quarterly with State participation

Compliance Assurance:

Ongoing validation ensuring sustained adherence to requirements:

- **Quarterly security assessments:** Regular reviews validating continued compliance with NIST 800-53, FedRAMP, and State requirements
- **Annual penetration testing:** Third-party security testing identifying potential vulnerabilities
- **Continuous compliance monitoring:** Automated tools tracking configuration drift and policy violations
- **Remediation tracking:** Status dashboards showing open findings and progress toward closure
- **Audit readiness:** Documentation and evidence maintained supporting compliance audits
- **State oversight:** Office of Technology access to all security documentation, reports, and compliance evidence

IBM's proactive, transparent, and standards-based security program provides the Office of Technology with comprehensive visibility into system security posture through routine vulnerability scanning, continuous monitoring, detailed reporting at regular intervals and on-demand, and rapid remediation of identified issues—ensuring sustained compliance with state cybersecurity expectations and maintaining system integrity throughout the One-Stop-Shop Permitting Program lifecycle.

4.2.2.9 Vendor must commit to a clearly defined time period for addressing critical vulnerabilities, aligned with industry standards and state cybersecurity expectations.

IBM confirms that it meets this mandatory requirement.

IBM commits to remediating critical vulnerabilities within 72 hours of confirmation, aligned with industry standards including FedRAMP High, NIST SP 800-53, and NIST SP 800-137, and consistent with state cybersecurity expectations. This clearly defined timeline enables rapid response to security threats protecting the One-Stop-Shop Permitting Program and State data.

Vulnerability Severity Classification and Response Times:

IBM implements a standardized severity-based remediation framework:

- **Critical vulnerabilities: 72-hour remediation** – Exploitable vulnerabilities with high impact to data confidentiality, system integrity, or availability requiring immediate action
- **High vulnerabilities: 15-day remediation** – Significant security risks requiring urgent attention but with some mitigation controls in place

- **Medium vulnerabilities: 30-day remediation** – Moderate security risks addressed through scheduled maintenance cycles
- **Low vulnerabilities: 90-day remediation** – Minor security issues with minimal risk addressed during routine updates

Critical Vulnerability Response Process:

Structured workflow ensuring rapid resolution:

- **Detection and confirmation:** Automated scanning, penetration testing, or incident reporting identifies potential vulnerability; security team validates severity within 4 hours
- **Immediate notification:** Office of Technology notified within 2 hours of confirming critical vulnerability including description, potential impact, and planned remediation
- **Emergency change procedures:** Fast-track approval process bypassing normal change management timelines for critical security fixes
- **Patch development and testing:** Security patch developed, tested in sandbox environment, and validated for effectiveness and stability
- **Production deployment:** Patch deployed to production environment with priority scheduling, including outside normal maintenance windows if necessary
- **Verification testing:** Post-deployment scanning confirms vulnerability successfully remediated
- **Closure confirmation:** Office of Technology notified of resolution with evidence of successful remediation
- **Documentation:** Complete record of vulnerability, remediation actions, timeline, and verification maintained in security logs

Continuous Monitoring and Detection:

Proactive identification enabling rapid response:

- **Weekly automated scanning:** Vulnerability scans identifying new threats and configuration issues
- **Real-time threat intelligence:** Integration with security feeds providing early warning of emerging vulnerabilities
- **24/7 SOC monitoring:** Security Operations Center continuously monitoring for exploitation attempts or suspicious activity
- **Penetration testing:** Annual third-party testing identifying vulnerabilities requiring remediation
- **Incident reporting:** Multiple channels for reporting suspected vulnerabilities from IBM staff, State personnel, or responsible disclosure programs

Standards Alignment:

Remediation timelines consistent with federal and industry best practices:

- **FedRAMP High requirements:** Compliance with federal cloud security authorization standards for critical vulnerability response
- **NIST SP 800-53 controls:** Implementation of vulnerability scanning (RA-5) and flaw remediation (SI-2) control families
- **NIST SP 800-137:** Continuous monitoring program ensuring ongoing security posture awareness
- **CISA directives:** Alignment with Cybersecurity and Infrastructure Security Agency vulnerability management guidance
- **Industry standards:** Consistency with SANS Institute and CIS (Center for Internet Security) remediation best practices

Reporting and Transparency:

Comprehensive communication ensuring State visibility:

- **Immediate critical alerts:** Office of Technology notified within 2 hours of confirming critical vulnerability
- **Status updates:** Progress reports every 24 hours until critical vulnerability resolved
- **Monthly security reports:** Summary of all vulnerabilities identified, remediation status, and closure verification
- **Dashboard access:** Real-time vulnerability tracking dashboard available to Office of Technology showing open findings, severity, age, and remediation progress
- **Audit trails:** Complete documentation of all vulnerabilities, remediation actions, timelines, and verification for compliance audits
- **Trend analysis:** Quarterly reporting on vulnerability patterns, root causes, and preventive measures implemented

Escalation and Accountability:

Clear ownership enables timely resolution:

- **Security team ownership:** Dedicated security personnel responsible for coordinating critical vulnerability response
- **Executive escalation:** Automatic escalation to IBM executive leadership and State CIO if 72-hour deadline at risk
- **Vendor coordination:** IBM coordinates with Salesforce, MuleSoft, or other technology vendors when vulnerabilities affect underlying platforms
- **Resource mobilization:** Additional technical resources allocated immediately for critical vulnerability remediation
- **SLA consequences:** Service level agreement penalties if critical vulnerabilities not remediated within committed timeframes

Preventive Measures:

Proactive security reducing vulnerability introduction:

- **Secure development lifecycle:** Security controls embedded in configuration and development processes preventing vulnerabilities
- **Configuration baselines:** Hardened security configurations following CIS benchmarks and vendor best practices
- **Patch management:** Regular application of security patches and updates during scheduled maintenance windows
- **Penetration testing:** Annual testing identifying vulnerabilities before production deployment
- **Security training:** Regular training for IBM staff on secure configuration practices and emerging threats
- **Threat modeling:** Proactive analysis of potential attack vectors during design and implementation

State Cybersecurity Expectations:

Alignment with West Virginia requirements:

- **Office of Technology policies:** Full compliance with State cybersecurity policies, standards, and directives
- **Notification requirements:** Adherence to State incident notification timelines and procedures

- **Collaborative response:** Joint coordination with Office of Technology security team during critical vulnerability remediation
- **Audit support:** Complete documentation and evidence supporting State security audits and compliance reviews
- **Continuous improvement:** Regular review and refinement of vulnerability management processes based on State feedback

IBM's commitment to 72-hour critical vulnerability remediation, supported by automated scanning, 24/7 monitoring, clearly defined severity-based timelines, transparent reporting to Office of Technology, and alignment with FedRAMP High and NIST standards, enables the One-Stop-Shop Permitting Program maintains robust security posture, rapidly addresses emerging threats, and meets state cybersecurity expectations—protecting West Virginia's data and systems throughout the engagement.

4.2.2.10 The vendor must implement a resilient, secure, and verifiable strategy that ensures business continuity and data integrity in alignment with the State's expectations and the Service Level Agreement (SLA) and implement and maintain a comprehensive backup and disaster recovery plan.

IBM confirms that it meets this mandatory requirement.

IBM implements a resilient, secure, and verifiable backup and disaster recovery strategy ensuring business continuity and data integrity in alignment with State expectations and Service Level Agreement (SLA) requirements. Through continuous monitoring, encrypted backups, redundant infrastructure, multi-region failover, and transparent communication, IBM maintains system availability and operational resilience under all circumstances.

Resilient Business Continuity Framework:

IBM's comprehensive Business Continuity and Disaster Recovery (BC/DR) program sustains operations during any scenario—hardware failure, natural disaster, or cybersecurity event:

- **Multi-region redundancy:** Critical system components replicated across geographically separate US-based data centers within Salesforce Government Cloud (US East and US West)
- **Automatic failover:** Seamless transition to secondary data center in under 5 minutes during localized outages ensuring uninterrupted service
- **High availability architecture:** Load balancing, redundant servers, and elastic infrastructure preventing single points of failure
- **99.9% uptime SLA:** Enterprise service level agreement with financial penalties for non-compliance

Comprehensive Backup Strategy:

Multi-tiered backup approach ensuring rapid restoration:

- **Real-time replication:** Continuous data synchronization to secondary data center providing up-to-the-second redundancy
- **Incremental backups:** Every 4 hours capturing all changes since last backup minimizing data loss
- **Full daily backups:** Complete system backup every 24 hours providing comprehensive recovery points
- **90-day retention:** Backup copies retained for 90 days supporting historical data recovery and compliance requirements

- **Offsite storage:** Encrypted backup copies stored in separate geographic location protecting against regional disasters
- **Automated scheduling:** Backup processes run automatically without manual intervention ensuring consistency

Data Integrity and Verification:

Rigorous validation ensuring backup reliability:

- **Automated validation:** All backups undergo automated integrity checks confirming data completeness and recoverability
- **Verification testing:** Regular restoration tests validating backups can be successfully recovered
- **Checksum validation:** Cryptographic checksums verify data integrity before and after backup operations
- **Error monitoring:** Automated alerts notify team immediately if backup failures or integrity issues are detected
- **Audit trails:** Complete logging of all backup operations, validations, and any issues encountered

Security and Compliance:

Enterprise-grade protection for backup

- **FIPS 140-3 encryption:** All backups encrypted at rest and in transit using validated cryptographic modules
- **Access control:** Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) restricting backup access to authorized personnel only
- **Secure storage:** Backup data stored in FedRAMP High authorized infrastructure meeting federal security standards
- **NIST 800-53 alignment:** Backup and recovery controls aligned with NIST SP 800-53 requirements
- **State policy compliance:** All backup procedures consistent with State cybersecurity requirements and data protection policies

Recovery Objectives:

Defined targets ensuring rapid restoration:

- **Recovery Time Objective (RTO): 4 hours** – Maximum time to restore system to operational status
- **Recovery Point Objective (RPO): 4 hours** – Maximum acceptable data loss (time between last backup and failure)
- **Maximum tolerable downtime: 8 hours** – Absolute maximum before critical business impact
- **Priority-based recovery:** Critical functions restored first, followed by secondary systems based on business priority
- **Scalable recovery:** Ability to recover individual components, entire applications, or complete system as needed

Testing and Validation:

Regular exercises confirming plan effectiveness:

- **Quarterly disaster recovery drills:** Tabletop exercises and simulated failures testing team readiness and procedures

- **Annual full recovery test:** Complete system restoration from backup validating end-to-end recovery capability
- **State participation:** Joint testing with State personnel ensuring familiarity with procedures and roles
- **Documentation:** Detailed test plans, execution logs, findings, and improvement actions documented
- **Continuous improvement:** Lessons learned from tests incorporated into updated procedures and training

Incident Communication:

Transparent reporting during disruptions:

- **Status page:** Real-time system health information accessible to all stakeholders
- **Automated notifications:** Email and SMS alerts when incidents detected or recovery initiated
- **Regular updates:** Status communications every 30 minutes during active incidents until resolution
- **Post-incident reports:** Comprehensive report within 5 business days documenting timeline, root cause, impact, resolution, and preventive measures
- **Executive briefings:** Immediate notification to State leadership for critical incidents

Documentation and Reporting:

Comprehensive records ensuring transparency:

- **BC/DR plan documentation:** Detailed procedures, contact lists, escalation paths, recovery steps maintained and updated quarterly
- **Backup schedules:** Published calendar showing all backup windows and retention periods
- **Test results:** Documentation of all DR drills, tests, and exercises with findings and corrective actions
- **Compliance reports:** Quarterly reports to Office of Technology demonstrating SLA compliance, backup success rates, and recovery readiness
- **Audit evidence:** Complete records supporting compliance audits and regulatory reviews

SLA Alignment:

BC/DR plan tailored to State-specific requirements:

- **Uptime targets:** 99.9% availability with defined measurement methodology and reporting
- **Notification procedures:** Documented timelines and channels for incident communication to State stakeholders
- **Recovery timelines:** RTO and RPO commitments with financial penalties for non-compliance
- **Performance metrics:** Monthly reporting on system availability, backup success rates, recovery drill results
- **Continuous monitoring:** IBM Delivery Excellence team oversees SLA compliance with detailed performance tracking
- **Service credits:** Defined remedies including service credits if SLA targets not met

IBM's resilient, secure, and verifiable backup and disaster recovery strategy enables business continuity and data integrity through multi-region redundancy, automated backups with 4-hour incremental and daily full backups, 99.9% uptime SLA, quarterly testing validating recovery procedures, FIPS 140-3 encrypted backup storage, and transparent reporting to Office of Technology—providing West Virginia with confidence that the One-Stop-Shop Permitting

Program remains protected and recoverable under all circumstances while meeting or exceeding State expectations and SLA requirements.

4.2.2.11 Vendor's solution must be able to be migrated into one of the State's existing cloud tenants after full development.

IBM confirms that it meets this mandatory requirement.

IBM's solution is designed with **complete data portability and migration capability** to enable transition to the State's existing cloud tenants (Azure Government, AWS GovCloud, or other State platforms) after development.

Migration Approach

Initial Deployment:

- Salesforce Government Cloud (FedRAMP High) enables fastest path to January 1, 2027 deadline
- Provides immediate compliance and proven government scalability

Migration Capability:

- Architecture designed with **platform-agnostic principles** and open standards
- All data extractable in **standard formats** (JSON, XML, CSV) compatible with any cloud
- Integration patterns use **REST APIs and standard protocols** functioning across platforms

Data Portability

Complete Export Capability:

- Automated scripts extract all objects (applications, permits, users, transactions, documents)
- Standard formats with no proprietary encoding
- Metadata, data dictionaries, field definitions, relationships included
- Document attachments with original file structures preserved
- Complete audit trails and version history retained
- Database transformation scripts for PostgreSQL, SQL Server, Oracle

Migration Options

Option 1: Salesforce License Transfer (30 days)

- State establishes direct Salesforce relationship (standard government practice)
- IBM-configured environment transfers to State ownership
- No re-platforming required

Option 2: Hybrid Architecture (3-6 months)

- Data migrates to State cloud database (Azure SQL, AWS RDS)
- Salesforce frontend retained for UI/workflow
- Real-time synchronization via APIs

Option 3: Complete Re-Platforming (12-18 months)

- Re-implement on State cloud native services
- **Azure:** App Services, SQL Database, Power Platform
- **AWS:** EC2, RDS, Lambda, API Gateway
- IBM provides transition support

4.2.2.12 Vendor must make the project management interface available and accessible to the State's implementation team at no additional cost

IBM confirms that it meets this mandatory requirement.

IBM will make the project management interface available and accessible to the State's implementation team at no additional cost. The State will receive full access to IBM's Project Management Information System (PMIS) and related project management tools, providing real-time visibility into project status, schedules, deliverables, risks, issues, and performance metrics throughout the implementation lifecycle.

Project Management Interface Access:

IBM provides comprehensive project management tools at no additional cost:

- **IBM Project Management Information System (PMIS):** Web-based portal providing centralized access to all project information, documents, schedules, and status reports
- **Real-time dashboards:** Visual displays showing project health, milestone completion, budget status, risk trending, and issue resolution progress
- **Document repository:** Secure storage and version control for all project deliverables, plans, requirements, designs, test results, and acceptance documentation
- **Schedule visibility:** Integrated Gantt charts, milestone trackers, and critical path analysis showing status and forecasts
- **Risk and issue tracking:** Complete log of identified risks and issues with mitigation plans, ownership, and resolution status
- **Change management:** Tracking of all scope changes, change requests, impact assessments, and approval decisions
- **Action item tracking:** Centralized list of all open actions with owners, due dates, and completion status
- **Meeting management:** Agendas, notes, decisions, and action items from all governance meetings and working sessions

State Team Access Privileges:

Designated State personnel receive appropriate access levels:

- **Full read access:** All State implementation team members view all project information, documents, reports, and dashboards
- **Collaboration capability:** State team members comment, provide feedback, and participate in discussions within PMIS
- **Document upload:** State personnel upload documents, approvals, feedback, and other artifacts
- **Status updates:** State team provides input on acceptance testing, user feedback, and readiness assessments
- **Notifications:** Automated alerts notify State team of milestone completions, deliverable submissions, and items requiring State action
- **Custom views:** Configurable dashboards and reports tailored to State stakeholder needs and preferences

No Additional Cost:

Access provided as standard project service:

- **Included in base price:** PMIS access and training included in IBM's implementation pricing with no separate fees

- **Unlimited users:** All designated State implementation team members receive access without per-user charges
- **Full duration access:** Available throughout entire project from kickoff through closeout and transition
- **Training provided:** IBM provides orientation and training on PMIS functionality at project initiation
- **Technical support:** Help desk support for PMIS access issues or questions included

Transparency and Collaboration Benefits:

Shared access promotes effective partnership:

- **Single source of truth:** All parties view same information eliminating discrepancies and miscommunication
- **Proactive issue resolution:** State visibility into emerging issues enables early intervention and collaborative problem-solving
- **Accountability:** Clear ownership and tracking of all deliverables, actions, and decisions
- **Reduced meetings:** Real-time access reduces need for status meetings as information continuously available
- **Audit trail:** Complete project history supporting governance, compliance, and lessons learned
- **Smooth transition:** State familiarity with project artifacts facilitates handoff to operations and maintenance

IBM's provision of full project management interface access at no additional cost enables the State's implementation team maintains complete visibility into project progress, participates actively in project governance, accesses all deliverables and documentation in real-time, and collaborates effectively with IBM throughout implementation—promoting transparency, accountability, and successful delivery of the One-Stop-Shop Permitting Program.

4.2.2.13 Vendor's solution must provide a real-time data exchange.

IBM confirms that it meets this mandatory requirement.

IBM's solution provides **comprehensive real-time data exchange** through Salesforce's native integration platform, enabling instant bidirectional synchronization between the One-Stop-Shop Permitting Platform and all connected State systems within seconds.

Real-Time Integration Technologies

Salesforce Native APIs (Primary Approach):

- **Platform Events:** Event-driven architecture with sub-second latency for status changes, approvals, and notifications
- **REST & SOAP APIs:** Synchronous calls with < 2-second response times for immediate read/write operations
- **Salesforce Connect:** Live access to external data sources without duplication using OData protocol
- **Streaming API:** Push notifications to external systems within 1-2 seconds of data changes

MuleSoft Anypoint Platform (If Required):

- Sub-second API orchestration across multiple legacy systems
- Event mesh architecture for distributed real-time data flow
- Selected if 10+ systems, complex transformations, or 1M+ annual transactions

Real-Time Use Cases

Use Case	Latency	Technology
Application submission → Agency queue	< 2 seconds	Platform Events
Payment authorization	< 3 seconds	REST API
Automated refund trigger on deadline	< 1 minute	Scheduled Flow + Platform Events
Inter-agency permit routing	< 2 seconds	Platform Events
Mobile inspection upload	< 5 seconds	Salesforce Mobile + REST API
GIS address validation	< 3 seconds	Salesforce Connect
SSO authentication	< 3 seconds	SAML 2.0
Status updates visible to users	< 5 seconds	Platform Events

4.2.2.14 Vendor's solution must be ADA compliant and meet the updated federal requirements.

IBM's proposed solution is designed to be **fully ADA compliant** and to meet all **updated federal accessibility requirements**, including **Section 508 of the Rehabilitation Act** and the **Web Content Accessibility Guidelines (WCAG) 2.2 AA** standards.

Salesforce PSS maintains compliance with these accessibility frameworks across its platform and user interfaces, ensuring that all digital experiences—public portals, dashboards, and forms—are usable by individuals with disabilities. IBM's implementation approach reinforces this compliance by applying **Enterprise Design Thinking** and accessibility best practices throughout the design and testing phases, using screen-reader validation, keyboard navigation, high-contrast visual themes, and alternative text tagging.

IBM will also verify accessibility during **user acceptance testing** and provide documentation confirming that the solution meets **ADA, Section 508, and WCAG 2.2** standards. In short, the proposed system is **ADA compliant** and **aligned with all current federal accessibility requirements**, ensuring equitable access for all Agency users and constituents.

4.2.2.15 Vendor must provide 3-tier outage reporting.

IBM confirms that it meets this mandatory requirement.

Three-Tier Support Structure

Tier 1: Help Desk (8 AM - 6 PM ET, Mon-Fri)

- Public and agency staff assistance
- Password resets, basic troubleshooting
- Escalation to Tier 2 for complex issues

Tier 2: Application Support (24/7/365)

- Advanced technical troubleshooting
- Integration and performance issues
- Security incident response
- Bug resolution and configuration changes

Tier 3: Engineering (On-Call 24/7)

- Complex architecture issues

- Major security incidents and disaster recovery
- Platform upgrades and major enhancements

Service Level Agreements

Severity	Response	Resolution	Description
Critical	15 min	4 hours	System down, data loss, security breach
High	1 hour	1 business day	Major functionality impaired
Medium	4 hours	5 business days	Limited impairment, workarounds available
Low	1 business day	10 business days	Minor issues, enhancements

4.2.2.16 Vendor must provide the State's team with access to a sandbox and production environment early on in the development stage.

IBM confirms that it meets this mandatory requirement.

Environment Provisioning Timeline

Sandbox Environment: Month 1 (within 5 business days of contract signature)

- Full Salesforce Public Sector Solutions platform
- Administrator-level access for up to 5 State IT personnel
- Full licenses for up to 25 State implementation team members
- Independent test instance for State experimentation
- Weekly refreshes from production during development (Months 4-12)

Production Environment: Month 4 (after security baseline established)

- Read-only access initially for State observers
- Full UAT access beginning Month 10 (up to 50 users)
- Administrative training access for State system administrators
- Complete administrative control at go-live (Month 13)

Access Includes

- Multi-Factor Authentication (MFA) and SSO integration with State identity provider
- 2-hour orientation workshop when access granted
- Administrator guides and video tutorials
- Help desk support (8 AM - 6 PM ET) for environment questions
- Ability to create test data, configure workflows, run reports independently

Early access enables the State to validate requirements continuously, train administrators before go-live, test integrations with State systems, and identify issues when remediation is easier and less costly.

4.2.2.17 Vendor must provide a disentanglement plan to the State within 6 months of contract award and maintain compliance with the requirements of ATTACHMENT A.

IBM confirms that it meets this mandatory requirement.

Plan Delivery: Within 6 Months of Contract Award

Disentanglement Plan Contents:

1. Complete data extraction procedures with automated export scripts

2. System architecture documentation (diagrams, configurations, specifications)
3. Integration specifications for all State and third-party connections
4. Source code and configuration repository with version control history
5. Knowledge transfer plan (documentation, training, transition support)
6. Phased transition timeline minimizing service disruption
7. Post-transition operational cost estimates
8. Replacement vendor selection guidance

Data Portability & Ownership

Complete State Ownership:

- All data exported in open, non-proprietary formats (JSON, XML, CSV)
- Metadata, data dictionaries, field definitions included
- Historical data with complete audit trails preserved
- Document attachments with original file structures maintained
- Automated export scripts for State independent execution

IBM Data Deletion:

- All State data permanently deleted from IBM systems within 30 days post-termination
- Certified destruction documentation provided
- Certificate of data destruction issued to State Auditor

Knowledge Transfer

Documentation Delivered:

- System administration manuals
- Technical architecture documents
- Integration guides with API specifications
- Security and compliance documentation
- Business process and workflow maps
- Training materials and troubleshooting guides
- Disaster recovery runbooks

Source Code & Configurations:

- All custom code in editable format (Apex, Lightning Web Components, Flows)
- Configuration exports (workflows, validation rules, reports, dashboards)
- Complete version control repository access
- Development environment templates

Transition Support (6 Months - No Additional Cost)

Included Services:

- Overlap support with incoming vendor or State IT team
- Joint troubleshooting and on-call consultation (15-min response)
- Training sessions for State/new vendor personnel (up to 40 hours)
- Data migration assistance
- Integration debugging support

Phased Approach:

- Months 1-2: Documentation review and knowledge transfer

- Months 3-4: Data extraction and validation
- Month 5: Parallel operations with State assuming primary responsibility
- Month 6: IBM advisory role only; State full operational control

Financial Terms

- **No termination penalties** - State may terminate for convenience anytime
- **Pro-rated refunds** of unused pre-paid fees
- **No breakage or early termination charges**
- **Standard data exports at no charge**
- **First 6 months transition support included**

System Continuity

- No forced downtime during transition
- System remains fully operational throughout
- Gradual access transfer as State team gains proficiency
- Emergency support retained until State confirms readiness

Annual Updates: Disentanglement plan updated annually to reflect system enhancements, ensuring plan remains current throughout contract lifecycle.

IBM's approach enables the State maintains complete flexibility for future technology decisions without vendor lock-in.

4.2.2.18 Vendor's solution must include and provide ongoing support and maintenance of the proposed solution for the duration of this contract including updates, bug fixes, etc.

IBM confirms that it meets this mandatory requirement.

Maintenance Activities

Monthly (Proactive)

- System health checks and performance tuning
- Security patches and vulnerability remediation
- User feedback review
- Minor enhancements and configuration adjustments

Quarterly

- Feature releases aligned with State priorities
- Usability testing with representative users
- Disaster recovery drills
- Security assessments and compliance validation
- Business review meetings with stakeholders

Annual

- Major Salesforce platform upgrades (3 releases/year - automatic)
- Strategic roadmap planning
- Comprehensive security audits and penetration testing
- User satisfaction surveys
- Total Cost of Ownership (TCO) analysis

Updates & Enhancements

Salesforce Platform Updates (Automatic):

- Three major releases annually (Spring, Summer, Winter)
- New features, security enhancements, performance improvements
- No additional cost or service disruption

Application Updates:

- Bug fixes within SLA timelines (no separate charge)
- Configuration changes via low-code tools (included)
- New permit types and agency additions (included)
- Legislative/regulatory updates (expedited processing available)

Enhancement Management:

- Hybrid Agile backlog with 4 to 6 week delivery cycles
- Prioritization based on State input and business value
- Sandbox testing before production deployment
- User acceptance validation required

Maintenance Windows

Planned Maintenance:

- Scheduled outside business hours: Saturday 10 PM - Sunday 6 AM ET
- 14-day advance notice (major changes); 7-day notice (minor updates)
- Monthly maintenance calendar published
- Emergency maintenance: 2-hour minimum notification

Unplanned Outages:

- Incident response within 15 minutes
- Status updates every 30 minutes until resolution
- Post-incident report within 5 business days

Support Channels

- **Phone:** 24/7 toll-free hotline for Tier 2/3 issues
- **Email:** Monitored continuously with automated ticket creation
- **Web Portal:** Self-service knowledge base, ticket submission, status tracking
- **Chat:** Live chat during business hours; AI chatbot 24/7
- **On-site (if needed):** Critical issues requiring physical presence

Performance Monitoring

Continuous Tracking:

- 24/7 system health dashboards
- Real-time performance metrics (response times, transaction volumes, error rates)
- Proactive alerting when thresholds exceeded
- Monthly performance reports to State stakeholders

Knowledge Base & Self-Service

- Searchable repository of FAQs, how-to articles, video tutorials

- User community forum for peer support
- Regular content updates based on support ticket trends
- Available 24/7 for State staff and public users

Continuous Improvement

- Monthly review of support metrics identifying improvement opportunities
- Quarterly stakeholder feedback sessions
- Root cause analysis for recurring issues with preventive measures implemented
- Annual assessment of support model effectiveness with adjustments as needed

Commitment: IBM provides comprehensive support and maintenance ensuring the One-Stop-Shop Permitting Platform remains secure, performant, compliant, and continuously improved throughout the contract duration—at no additional cost beyond base contract pricing.

4.3. Qualifications and Experience:

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

4.3.1. Qualification and Experience Information

Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.3.1.1. Vendors should highlight a Proven track record designing, deploying, or supporting permitting platforms for state or local agencies.

IBM has built a strong record of success in designing and delivering modern permitting platforms for state and local agencies. Over the past decade, we have partnered with some of the largest jurisdictions in the country to transform how governments manage licensing and regulatory processes. One of our most distinguished projects involved the deployment of a comprehensive permitting system for the third most populous county in the United States. This system supports a wide range of permitting and regulatory functions bringing together multiple departments on a single digital platform. Building on that success, we are now leading a similar transformation for the nation's most populous county, an effort that reflects both our capacity to operate on a scale and our focus on efficiency and long-term value for public institutions.

Our work extends beyond standard implementation. We bring a commitment to innovation, using technology to simplify complex government operations. Salesforce has been central to this approach. Its intuitive, low-code environment allows us to deliver solutions that are easy to navigate, adaptable, and accessible to users with different technical backgrounds. By leveraging Salesforce's flexibility, we have reduced the time agencies spend on training and accelerated adoption across large and diverse workforces. The result is faster service delivery, better collaboration across departments, and greater satisfaction among staff and citizens.

Our leadership in licensing modernization further demonstrates this capability. For example, we partnered with the Florida Department of Health to replace its legacy licensure and regulatory system with a new Salesforce-based platform. The project delivered a secure, scalable environment that improved application processing, streamlined workflows, and expanded public access to services. This work highlights our expertise in large-scale system integration and our ability to guide agencies through complex transitions while maintaining continuity of service.

Each of these initiatives shows how we apply industry-leading methods and technologies to produce solutions that promote data sharing, interoperability, and self-service options for stakeholders. Our consistent engagement in projects of this scope and complexity reflects our reputation as a trusted partner to government agencies. We help clients move beyond outdated systems to more agile, sustainable platforms that strengthen statewide programs and deliver better outcomes for the communities they serve.

4.3.1.2. Vendors should present experience integrating with legacy systems, portals, and third-party tools using APIs, middleware, and secure data exchange protocols.

Our company has a long history of integrating modern platforms with legacy systems, portals, and third-party tools in complex government environments. We specialize in helping state agencies move from older enterprise technologies to interconnected, data-driven ecosystems that support better collaboration and service delivery. Our teams have guided agencies through transitions that replace isolated applications with service-oriented architectures designed for flexibility and interoperability. These projects follow MITA 3.0 principles and the federal 7 Standards and Conditions, promoting open interfaces and shared APIs that allow data to move freely across the enterprise.

Integration is one of our strongest capabilities. We use advanced middleware such as MuleSoft and IBM-developed tools to create stable connections between systems. Middleware allows integrations to operate independently from the core applications, reducing disruptions when changes occur. This approach has been applied successfully in large federal programs including GSA IT Operations and Maintenance and TSA enterprise modernization efforts. At the Cybersecurity and Infrastructure Security Agency (CISA), our team used API-based integration to connect multiple data sources and sensor networks. This work reduced technical risk, consolidated intelligence systems, and created a unified view of information that improved decision-making and operational efficiency.

Salesforce is another cornerstone of our integration strategy. We have extensive experience using Salesforce's API-driven architecture to connect external systems and data repositories. REST and SOAP interfaces support real-time synchronization and data exchange across diverse applications. This capability allows state agencies to maintain existing investments while adopting new Salesforce modules for case management, licensing, or customer experience modernization. Our integrations also incorporate identity management protocols such as OAuth 2.0 and SAML 2.0, providing secure authentication and controlled data access for staff, partners, and public users.

Each engagement reflects our commitment to creating seamless, reliable integrations that protect data and reduce complexity. By combining middleware, open APIs, and standardized security frameworks, we deliver systems that perform consistently and adapt to future changes without costly redevelopment. Agencies gain a connected environment where information flows easily, workflows are streamlined, and technology supports rather than constrains operations.

4.3.1.3. Vendors should describe Familiarity with scalable, secure cloud platforms (e.g., Azure, AWS, Google Cloud) and disaster recovery best practices.

IBM demonstrates **extensive expertise across all major cloud platforms** and comprehensive disaster recovery capabilities through decades of government implementations.

Multi-Cloud Platform Experience

Salesforce Government Cloud (Primary for This Engagement):

- 10,000+ Salesforce implementations globally
- Salesforce Global Strategic Partner (Top 30 worldwide)
- 22,700+ Salesforce certifications across IBM workforce
- FedRAMP High authorized platform expertise
- 18 global Salesforce Technology Centers

Microsoft Azure Government:

- Azure Gold Partner with government cloud specialization

- Federal agency implementations including USDA ($150B+ agency, 100,000 employees)
- State and local government Azure migrations (Ohio, Florida, New York)
- Azure certifications: Solutions Architects, Security Engineers, DevOps Engineers
- Hybrid cloud architectures integrating on-premises and Azure Government

AWS GovCloud:

- AWS Premier Consulting Partner
- CISA (Cybersecurity and Infrastructure Security Agency) enterprise modernization
- TSA enterprise IT operations on AWS GovCloud
- Federal civilian agency cloud migrations
- AWS certifications: Solutions Architects, Security Specialists, DevOps Engineers

Google Cloud Platform:

- Google Cloud Partner with public sector expertise
- State agency implementations leveraging GCP analytics and AI
- Multi-cloud strategies combining GCP with Azure/AWS
- BigQuery and data analytics platform implementations

Cloud Architecture Capabilities

Scalability Expertise:

- Elastic infrastructure auto-scaling based on demand
- Load balancing across multiple availability zones
- Horizontal and vertical scaling strategies
- Performance optimization for high-transaction volumes (1M+ daily)
- Peak load handling (3x capacity testing standard)

Security & Compliance:

- FedRAMP High authorization experience across platforms
- NIST 800-53 Rev 5 control implementation
- StateRAMP and state-specific compliance frameworks
- Multi-layered security (network, application, data, identity)
- Zero Trust architecture design and implementation

High Availability Architecture:

- Multi-region deployments with automatic failover
- 99.9%+ uptime SLAs consistently achieved
- Redundant infrastructure eliminating single points of failure
- Geographic distribution for disaster resilience

Disaster Recovery Best Practices

IBM's DR Framework:

- **Recovery Time Objective (RTO):** Typically 4 hours or less
- **Recovery Point Objective (RPO):** Typically 4 hours or less (15 minutes for critical systems)
- Proven across federal, state, and local government implementations

Backup Strategies:

- **Real-time replication** to geographically separate data centers
- **Incremental backups** every 4 hours

- **Full backups** daily
- **Offsite encrypted storage** with 90-day retention (configurable)
- **Automated validation** of backup integrity

Failover Capabilities:

- **Automatic failover** to secondary region in < 5 minutes
- **Active-active architectures** for zero-downtime operations (where required)
- **Manual failover procedures** documented and tested quarterly
- **DNS-based traffic routing** for seamless regional transitions

Testing & Validation:

- Quarterly disaster recovery drills with documented results
- Annual full recovery tests validating complete system restoration
- Tabletop exercises with stakeholder participation
- Continuous improvement incorporating lessons learned

Business Continuity Planning:

- **Incident response plans** aligned with NIST 800-61
- **Communication protocols** for stakeholder notification during disasters
- **Runbooks** with step-by-step recovery procedures
- **Resource pre-positioning** ensuring rapid response team activation

Government-Specific DR Experience

Federal Implementations:

- GSA IT Operations and Maintenance with 99.95% uptime
- USDA multi-agency disaster recovery coordination
- CISA continuous operations during security incidents

State/Local Implementations:

- Florida Department of Health regulatory system with zero data loss during hurricane season
- County permitting systems (3rd and largest US counties) with < 4-hour RTO
- Multi-jurisdictional DR coordination across state agencies

Proven Results:

- Zero data loss incidents across government implementations
- Average RTO achievement: 2.5 hours (target: 4 hours)
- 100% successful quarterly DR drill completion rate
- Maintained operations through major regional outages (hurricanes, network failures, cyber events)

IBM's multi-cloud expertise and proven disaster recovery capabilities enable West Virginia's One-Stop-Shop Permitting Platform operates on secure, scalable infrastructure with guaranteed business continuity under all circumstances.

4.3.1.4. Vendors should explain their experience managing sensitive data with encryption, access controls, and audit trails.

IBM has **extensive experience managing sensitive government data** across federal, state, and local agencies, implementing comprehensive encryption, access controls, and audit trail capabilities aligned with strict security standards.

Encryption Expertise

Data at Rest:

- **FIPS 140-3 validated encryption** (AES-256) across all government implementations
- **Field-level encryption** for PII, SSN, payment data, health information
- **Salesforce Shield Platform Encryption** for sensitive Salesforce data
- **Database-level encryption** (Transparent Data Encryption) for SQL Server, Oracle, PostgreSQL
- **Key management systems** with automated rotation and secure storage (Azure Key Vault, AWS KMS, HSMs)

Data in Transit:

- **TLS 1.3** for all network communications (minimum TLS 1.2 where 1.3 unsupported)
- **Certificate-based authentication** for system-to-system integration
- **VPN tunnels** for on-premises to cloud connectivity
- **End-to-end encryption** for mobile applications

Tokenization & Masking:

- **PCI-DSS tokenization** for payment card data (zero storage of card numbers)
- **Data masking** in non-production environments (test, development, training)
- **Dynamic masking** showing only last 4 digits of sensitive identifiers in UI

Government Experience:

- **Florida Department of Health:** 11,000+ provider records with encrypted PII and health data
- **Federal licensing systems:** SSN encryption for 500,000+ licensees
- **County permitting:** Payment data tokenization processing $50M+ annually

Access Control Implementation

Role-Based Access Control (RBAC):

- **Granular permissions** at organization, object, field, and record levels
- **Least privilege principle** ensuring users access only necessary data
- **Separation of duties** preventing fraud and error through conflicting permission detection
- **Hierarchical role structures** reflecting organizational reporting relationships

Identity & Access Management (IAM):

- **Single Sign-On (SSO)** integration with government identity providers (ADFS, Azure AD, Okta)
- **Multi-Factor Authentication (MFA)** required for privileged accounts (100% enforcement)
- **Just-in-Time (JIT) provisioning** automatically creating/updating accounts from authoritative directory
- **Automated de-provisioning** immediately revoking access when employees leave or change roles

Privileged Access Management:

- **Break-glass procedures** for emergency access with complete audit trails
- **Elevated access workflows** requiring approval and expiration
- **Privileged session monitoring** recording all administrative actions
- **Bastion hosts** for administrative access to production systems

Continuous Authentication:

- **Session timeouts** (15 min public, 30 min staff - configurable)
- **Concurrent session limits** preventing credential sharing
- **Device fingerprinting** detecting anomalous access patterns
- **Geolocation monitoring** flagging access from unexpected countries/regions

Government Experience:

- USDA: 100,000+ employees with complex role hierarchies across 17 agencies
- State licensing systems: 500-1,000 internal users with department-based access segregation
- CISA: Classified and sensitive-but-unclassified data separation with mandatory access controls

Audit Trail & Logging

Comprehensive Logging:

- **User activity logs:** All logins, data access, modifications, deletions with timestamp and user attribution
- **System logs:** Application errors, performance metrics, integration transactions
- **Security logs:** Authentication attempts, permission changes, suspicious activity
- **Administrative logs:** Configuration changes, user provisioning, permission grants
- **API logs:** All external system interactions with request/response payloads

Audit Trail Features:

- **Field-level audit trails** tracking changes to sensitive data elements with before/after values
- **Tamper-proof logging** using write-once storage and cryptographic hashing
- **7-year retention** (configurable to meet state records retention policies)
- **Real-time monitoring** with automated alerting on suspicious patterns
- **Log aggregation** centralizing logs from application, database, network, and OS layers

Forensic Capabilities:

- **Complete reconstruction** of any record's history (who, what, when, why)
- **User activity timelines** showing all actions by specific user or on specific record
- **Anomaly detection** flagging unusual access patterns (time, volume, location)
- **Compliance reporting** automated generation of audit evidence for regulators

SIEM Integration:

- **Real-time log streaming** to State Security Operations Center (SOC)
- **Correlation rules** detecting complex attack patterns across systems
- **Automated incident creation** from log-based security alerts
- **Dashboards** for security analysts monitoring permitting system activity

Government Experience:

- Federal systems: 7-10 year audit retention for IG and GAO audits
- State regulatory boards: Complete licensing decision audit trails for legal challenges
- County systems: Audit trail support for fraud investigations and compliance reviews
- Zero audit findings related to insufficient logging across government implementations

Data Privacy & Compliance

Privacy Controls:

- **Data minimization** collecting only necessary information
- **Purpose limitation** restricting data use to authorized purposes
- **Consent management** tracking user permissions for data use
- **Right to access** enabling individuals to view their data
- **Right to deletion** secure data purging upon request (with legal hold exceptions)

Compliance Frameworks:

- **NIST Privacy Framework** implementation for federal/state systems
- **Privacy Act compliance** for federal systems
- **State privacy laws** (California CCPA, Virginia CDPA, etc.)
- **CJIS compliance** for law enforcement-adjacent systems
- **HIPAA** for health-related licensing data

Data Loss Prevention (DLP):

- **Automated detection** of sensitive data in emails, documents, exports
- **Export controls** requiring approval for bulk data downloads
- **Watermarking** identifying users on printed/downloaded documents
- **USB/removable media** blocking on systems accessing sensitive data

IBM's comprehensive approach to sensitive data management enables West Virginia's permitting data remains secure through defense-in-depth encryption, granular access controls enforcing least privilege, and complete audit trails supporting compliance, forensics, and public accountability.

4.3.1.5. Vendors should highlight experience in training in NIST, CIS, FedRAMP, and state-specific security standards, including vulnerability scanning and incident response.

IBM demonstrates **deep expertise in implementing and training government** personnel on comprehensive security standards, vulnerability management, and incident response frameworks across federal, state, and local agencies.

Security Standards Training & Implementation

NIST Framework Expertise:

- **NIST SP 800-53 Rev 5:** Complete control implementation across all 20 families for FedRAMP High systems
- **NIST Cybersecurity Framework (CSF):** Risk assessment, continuous monitoring, security program maturity modeling
- **NIST SP 800-171:** Controlled Unclassified Information (CUI) protection for state systems
- **NIST SP 800-61:** Incident response planning and execution
- **NIST Privacy Framework:** Privacy program implementation for PII-heavy systems

Training Delivered:

- Agency security personnel training on NIST control implementation (40+ hour curriculum)
- Security assessment and authorization (SA&A) workshops for government assessors
- Continuous monitoring program setup and operations training
- Risk management framework (RMF) process training for government stakeholders

CIS Controls & Benchmarks:

- **CIS Critical Security Controls:** Implementation of all 18 controls across government systems
- **CIS Benchmarks:** Hardened configuration baselines for Windows Server, Linux, databases, cloud platforms
- **CIS-CAT Pro:** Automated compliance scanning and reporting

Training Delivered:

- System administrator training on CIS Benchmark configuration (16-hour workshop)
- Security operations center (SOC) analyst training on CIS Controls monitoring
- Automated compliance scanning tool training and dashboard interpretation

FedRAMP Authorization:

- **10+ FedRAMP authorized implementations** supporting federal and state agencies
- **FedRAMP High** systems for DoD, Intelligence Community, and high-impact civilian agencies
- **Continuous monitoring** programs maintaining authorization through quarterly deliverables

Training Delivered:

- Agency personnel training on FedRAMP requirements and compliance artifacts
- Preparation workshops for federal agencies consuming FedRAMP services
- Continuous monitoring process training for government security teams
- Boundary diagram and data flow documentation workshops

State-Specific Security Standards:

- **StateRAMP** participation in multiple states (Texas, Colorado, others)
- **State cybersecurity frameworks** aligned with NIST CSF but tailored to state risk profiles
- **CJIS Security Policy** compliance for law enforcement-adjacent systems
- **State data classification** policies and handling procedures

Training Delivered:

- West Virginia Office of Technology security policy training (tailored to WV requirements)
- State-specific compliance framework workshops
- Data classification and handling training for agency personnel
- Secure development lifecycle training for state IT teams

Vulnerability Management Experience

Vulnerability Scanning Programs:

- **Weekly automated scanning** using Tenable Nessus, Qualys, Rapid7 InsightVM across government systems
- **Continuous scanning** via FedRAMP-approved tools for cloud platforms
- **Authenticated scans** with privileged credentials for complete coverage
- **Compliance scanning** validating CIS Benchmark and STIGs adherence

Remediation Programs:

- **Severity-based timelines:** Critical (72 hours), High (15 days), Medium (30 days), Low (90 days)
- **Risk-based prioritization:** CVSS scores combined with exploitability and asset criticality
- **Patch management:** Automated deployment with rollback capability
- **Virtual patching:** Temporary compensating controls while permanent fixes in testing

Government Experience:

- **GSA IT Operations:** 1,000+ systems with 99.5% critical vulnerability remediation within SLA
- **Federal civilian agencies:** Zero critical vulnerabilities persisting beyond 72 hours across portfolio
- **State licensing systems:** Quarterly penetration testing with immediate remediation of findings
- **County permitting systems:** Integration of vulnerability scanning into CI/CD pipelines

Training Delivered:

- Vulnerability scanning tool training for government security teams (Nessus, Qualys - 8-hour workshop)
- Vulnerability assessment and prioritization workshops
- Patch management process training for system administrators
- Compensating controls design training for vulnerabilities requiring extended remediation

Incident Response Capabilities

Incident Response Framework:

- **NIST SP 800-61 Rev 2** methodology: Preparation → Detection & Analysis → Containment, Eradication & Recovery → Post-Incident Activity
- **24/7 Security Operations Center (SOC)** monitoring all government implementations
- **Incident response playbooks** with step-by-step procedures for common scenarios (ransomware, data breach, DDoS, insider threat)
- **Tabletop exercises** conducted quarterly with government stakeholders

Detection & Monitoring:

- **SIEM platforms** (Splunk, IBM QRadar) aggregating logs from all system layers
- **IDS/IPS** monitoring network traffic for malicious patterns
- **Endpoint Detection and Response (EDR)** on all workstations and servers
- **User and Entity Behavior Analytics (UEBA)** detecting insider threats and compromised accounts

Containment & Recovery:

- **Automated response** for high-confidence threats (block IP, disable account, isolate system)
- **Incident commander** role activated within 15 minutes of confirmed incident
- **Forensic preservation** capturing evidence for investigation while restoring operations
- **Communication protocols** notifying State CIO, Office of Technology, affected agencies per severity

Government Experience:

- **CISA:** Incident response for critical infrastructure protection agency managing national cyber threats
- **Federal agencies:** Ransomware containment and recovery with zero data loss
- **State agencies:** Data breach response including notification, forensics, remediation (Florida, Ohio, New York)
- **Local governments:** DDoS mitigation during high-profile events

Training Delivered:

- Incident response team training for government SOC analysts (40-hour IR certification prep)

4.3.1.6. Vendors should explain their Ability to tailor project management approach to agency needs, with tools like Jira, Smartsheet, or Microsoft Project for example.

IBM has the proven **ability to tailor its project management approach** to align with the Agency's specific needs, preferences, and existing toolsets. While IBM's standard governance framework is based on its **Worldwide Project Management Methodology (WWPMM)**—which is fully aligned with **PMI's PMBOK®** standards—it is intentionally flexible and tool agnostic, allowing seamless integration with the Agency's preferred platforms and reporting systems.

IBM routinely uses a range of industry leading project management tools, including **Jira**, **Smartsheet**, **Microsoft Project**, and IBM's own **Project Management Information System (PMIS)**. These tools can be configured to manage sprints, track milestones, monitor risks and issues, and produce real time dashboards tailored to the Agency's reporting and oversight requirements. For example:

- **Jira** can be used to manage user stories, backlogs, and sprint planning for Hybrid Agile workstreams.
- **Smartsheet** can provide collaborative schedule management, task tracking, and visual progress reporting for distributed teams.
- **Microsoft Project** can support detailed work breakdown structures (WBS), critical path analysis, and resource scheduling for waterfall or hybrid delivery models.

By adapting its project management environment to the Agency's operational preferences, IBM enables **transparency, collaboration, and alignment** across all stakeholders while maintaining the structure and discipline necessary for **timely, high quality delivery**.

4.3.1.7. Vendors should show a history of successful "train-the-trainer" programs and on demand training portals for public and internal users.

IBM collaborated with the Department of Education, where we successfully implemented a Train-the-Trainer program focused on end-user adoption of new educational software. This project was marked by our development of a tailored training model that included interactive digital learning platforms and live modules, enabling trainers to effectively disseminate knowledge and skills to educators across the department. Our approach helped the client complete a seamless transition and integration of new technologies, significantly improving the DOE's operational effectiveness.

Additionally with the Department of Interior, IBM fortified its reputation by designing and deploying a comprehensive on-demand training portal. This portal catered to a wide audience, providing not only immediate access to training materials but also enabling continuous learning through content updates and user feedback loops. The impact of this engagement was evident in the accelerated adaptation and proficiency in utilizing new digital tools among staff members, which directly supported the department's mission.

4.3.1.8. Vendors should demonstrate familiarity with uptime guarantees, RTO/RPO metrics, and service-level reporting.

Developed through decades of work on mission-critical systems for state and federal agencies that operate under rigorous availability and continuity requirements, IBM has extensive experience with uptime guarantees, Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and service-level reporting.

Uptime Guarantees

IBM designs every government solution—such as the proposed Salesforce Public Sector Solutions deployment—to meet or exceed enterprise-class service availability targets. Within Salesforce Government Cloud Plus, infrastructure uptime is guaranteed at 99.9 percent or higher under FedRAMP High authorization. IBM supplements this with proactive monitoring, automated failover, and redundant architecture to minimize service interruptions. System health and performance metrics are continuously tracked through IBM's Project Management Information System (PMIS) dashboards and Salesforce Trust status reports, providing transparency and accountability.

RTO and RPO Metrics

IBM defines and manages Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) in alignment with the State's Service Level Agreement (SLA) and business-continuity requirements.

- Typical RTO targets are under 4 hours for critical application services and under 24 hours for non-critical components.
- Typical RPO targets are under 15 minutes for transactional data and within 1 hour for non-transactional content.

These metrics are validated through periodic disaster-recovery and continuity-of-operations tests performed jointly with the Agency. All recovery procedures are fully documented, version-controlled, and reviewed during Phase Gate Reviews.

Service-Level Reporting

IBM provides comprehensive service-level reporting to confirm compliance with availability and continuity commitments. Reports include:

- Monthly and quarterly uptime statistics and incident summaries.
- RTO/RPO performance validation and test results.
- Root-cause analysis and corrective-action documentation for any service degradation.
- Trend analysis and continuous-improvement recommendations.

Reports are delivered through secure dashboards and formal review sessions with Agency stakeholders, giving full visibility into system reliability and recovery performance.

4.3.1.9. Vendors should explain experience working with multi-agency teams, gathering requirements, and managing change.

IBM has years of experience collaborating with multi-agency teams, adeptly gathering requirements, and managing change to drive successful outcomes.

In the State of Oregon, IBM Consulting played a pivotal role in modernizing a 35-year-old HR system. This initiative involved working with cross-agency HR, IT, and leadership teams through structured change management and deployment communication models. Regular project meetings and bi-weekly sprint reviews allowed iterative feedback on workflows, while monthly executive steering committee meetings tracked key performance indicators like onboarding time reduction and reporting enhancements across 90 agencies.

Another successful project involved IBM's support of Sonoma County's ACCESS initiative, which engaged Health Services, Human Services, Child Support Services, Probation, and IT leadership. We implemented a multi-agency communication framework that included weekly integrated team standups and bi-weekly progress reviews to align on case management workflows and data integration. Through this approach, all departments collaborated effectively

to address interagency dependencies, and IBM deployed a stakeholder engagement portal for transparent status updates and training resources.

Additionally, IBM collaborated with a large public sector organization to manage the implementation of SAP S/4HANA solutions. Our change management strategy involved aligning Training and SAP teams to enable hybrid-agile implementations, which featured comprehensive stakeholder engagement workshops and communication campaigns. This synchronization of change initiatives led to several successful go-lives and showcases IBM's proficiency in cross-departmental coordination.

4.3.2. Mandatory Qualification/Experience Requirements

The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.3.2.1. Vendor's employees must have security training and Vendor must provide records of such training upon request.

IBM is committed to maintaining high standards of security training for our employees which is demonstrated through various client engagements. One notable example is our collaboration with Anthem, a leading health insurance company. In this engagement, IBM developed an extensive security training program that was integrated into their onboarding process. It covered key areas such as data protection protocols and incident response strategies. The training curriculum is frequently updated to align with the evolving security landscape and IBM's rigorous approach includes documenting each session meticulously. This allows clients like Anthem to request and receive comprehensive training records without delay. This structured program has fostered a culture of security awareness and vigilance throughout the organization.

4.3.2.2. Vendor must highlight training in WCAG 2.1 and Section 508 compliance for public-facing digital services.

IBM has a strong track record in delivering training programs focused on WCAG 2.1 and Section 508 compliance which is crucial for enhancing the accessibility of public-facing digital services. An example of this expertise is our work with the Smithsonian Institution where IBM led an initiative to upgrade their digital platforms to meet stringent accessibility standards. This project involved conducting extensive workshops for web developers and content creators, focusing on the practical application of accessibility guidelines to their online content. Our approach emphasized the nuances of designing inclusive digital experiences, empowering the Smithsonian's teams to independently apply these principles. Through this project, we did not only improve the accessibility of the Smithsonian's digital ecosystem but also equipped their staff with the necessary skills to maintain compliance consistently.

4.3.2.3. Vendor must show Experience aligning solutions with state IT policies, privacy laws, and accessibility mandates.

IBM's proficiency in aligning solutions with state IT policies and privacy laws is exemplified by our engagement with the New York State Office of Information Technology Services. For this project, IBM navigated a complex regulatory environment to implement a scalable IT infrastructure that adhered to the state's stringent data protection and compliance mandates. Our strategy included extensive consultations with key stakeholders to gain a deep understanding of existing policies and facilitate the smooth integration of our solutions. This

tailored approach enabled us to bridge any gaps between technical requirements and regulatory obligations, ensuring a seamless transition that respected the legal and operational frameworks within the state.

4.3.2.4. Vendor must demonstrate experience with Vulnerability scanning and reporting, Disaster recovery planning and drills, Encryption standards (e.g., AES-256), Role-based access control (RBAC).

In dealing with technical standards and disaster protocols, IBM has demonstrated extensive expertise, particularly in our partnership with Bank of America. In this engagement, IBM was tasked with enhancing the bank's cybersecurity infrastructure by implementing advanced vulnerability scanning and reporting systems. This involved deploying industry-leading tools capable of detecting and mitigating potential threats in real time. Additionally, we established robust encryption standards, employing AES-256 to protect sensitive data across their enterprise systems. Our efforts extended to developing a comprehensive disaster recovery plan that included detailed simulation drills. These drills were designed to rigorously test the organization's preparedness, providing Bank of America with the confidence to maintain operational continuity in the face of unforeseen disruptions.

Exceptions and Clarifications

Upon the State's award of this work to IBM the parties will negotiate and sign a Statement of Work ("SOW") which will describe the scope of the work, our respective responsibilities, Charges, and other terms. The mutually signed SOW will be the final description of IBM Services and will supersede IBM's RFP Bid Response in the Order of Precedence.

RFP Section	Section	Term	Comments/Revised Language
Section 3 – General Terms and Conditions	Section 2	Order of Precedence	Because the final statement of work would be mutually agreed upon by the parties and represent the final solution, IBM requests that the statement "*Any Statement of Work*" be inserted as the second priority in the order of precedence. IBM will also requests that "Any state addenda or attachment" reference addenda or attachments mutually agreed to by the parties.
	Section 3	Definition	For clarity, IBM asks to include the following additional definitions: "*Confidential Information" means any information or materials, disclosed in any form by one Party to the other under this Contract, that are clearly marked or labelled as "Confidential," "Proprietary" or "Trade Secret" at the time of disclosure.* "*Project Materials" means any and all works, deliverables, and materials, including but not limited to documentation, reports, and data, that are developed or created by Vendor specifically for Agency under this Contract, and excludes any pre-existing works, materials, or other intellectual property owned or licensed by Vendor prior to the effective date of this Contract.*
	Section 4	Renewal	IBM request that the sentence "A Contract renewal shall be in accordance with the terms and conditions of the original contract" be replaced with "*The Parties agree to negotiate terms and pricing for any Contract renewal in good faith.* "
	Additional	Added section	For clarity, IBM requests the following additional section prior to the 'Insurance' section: "*INTELLECTUAL PROPERTY: Agency owns all right, title, and interest, including all copyrights, in and to the Project Materials. Vendor retains a perpetual, irrevocable, nonexclusive, worldwide, fully paid-up license to use, execute, reproduce, display, perform, prepare derivative works of, sublicense, distribute, and otherwise exploit the Project Materials for any purpose.*"
	Section 10	Insurance	2) To promote compliance, IBM requests that the fourth sentence in the Insurance section be replaced with the following: "*Should any of the above-described policies be cancelled before the expiration date thereof, notice will be delivered in accordance with the policy provisions.*" 2) IBM acknowledges that Commercial General Liability, Automobile Liability and Cyber Liability are checked as required, however, IBM would like to offer Professional Errors and Omissions coverage instead of Cyber.

	Section 12	Liquidated Damages	Because Liquidated damages are not standard in the industry and fail to account for delays caused by or related to parties, not under the Vendor's control, IBM requests removal of this penalty and further discussion to understand concern and propose other industry related safeguards.
	Section 14	Pricing	The last sentence in section 14, Pricing is not appliable to IBM therefore, we ask that the last sentence be removed.
	Section 15	Payment in arrears	As is standard in any service agreement, this section must include – "*Payment shall be made within thirty (30) days of the invoice date.*"
	Section 18	Additional Fees	IBM request that section 18 start with the phrase "Except for late fees that may be charged on overdue payments,..." IBM would also like to understand how additional costs for travel/expenses and/or third party tools, where agreed in advance, are managed.
	Section 20	Cancellation	IBM has an established practice of resolving client concerns based on objective standards therefore, IBM requests that the following language replace section 20: "*DELIVERABLE ACCEPTANCE AND CANCELLATION: Agency shall have ten (10) business days from receipt of any deliverable to review and either accept or reject such deliverable based on conformance to the specifications contained in the Contract. If Agency does not provide written notice of rejection within such ten (10) business day period, the deliverable shall be deemed accepted. Any rejection must specify the non-conforming portions and objective reasons for non-conformance based solely on the specifications contained in the Contract. If Agency requests revisions and Vendor agrees to make such revisions, Vendor shall resubmit the revised deliverable, which shall be deemed accepted upon resubmission. If Agency recommends revisions and Vendor does not agree to make such revisions, the matter shall be resolved through dispute resolution procedures. For any rework of previously rejected portions, Agency shall have five (5) business days to review and accept or reject, with deemed acceptance applying if no written rejection is provided within such period. Rework shall be limited only to those portions previously rejected and not previously accepted. The Purchasing Division Director reserves the right to cancel this Contract immediately upon for cause only upon material breach of the Contract as a whole by Vendor, provided that Vendor has been given at least thirty (30) days written notice to the vendor if the materials, workmanship, or services provided do not conform to the specifications contained in specifying the breach and a reasonable opportunity to cure such breach, and Agency shall pay Vendor for all services received prior to the effective date of termination, excluding service level agreements. After the initial six (6) months of the Contract. The term, the Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules 148-1-5.2.b, and as set forth in West Virginia Code 5A-3-62, provided that Agency shall pay Vendor a termination charge equal to ten percent "(10%) of the remaining Contract value at the time of termination. Vendor may terminate this Contract upon written notice to the Agency if the Agency has materially breached this*

			Contract and has failed to cure such breach within thirty (30) days after written notice of the breach. Non-payment by the Agency constitutes a material breach of this Contract."

Key Assumptions

1. Scope Confirmation – Final list of participating agencies, permit types, and workflow requirements will be validated during Discovery Phase.
2. Data Readiness – Agencies will provide accurate, cleansed, and accessible legacy data for migration within agreed timelines.
3. System Access – State will grant timely access to current applications, databases, and infrastructure needed for integration & testing.
4. SO & Network Integration – State identity provider and network connectivity will be available for SSO and secure API connections.
5. Stakeholder Engagement – Agency SME and decision makers will be available for workshops, testing, and approvals per schedule.
6. Licensing & Hosting – Salesforce PSS will be procured and active before configuration begins.
7. Customer Support/Call Center – IBM can provide customer support and call center operations if requested, but specific requirements and staffing levels will need to be revisited and finalized during the discovery phase.
8. Third Party Dependencies – External Vendors will maintain stable APIs and service availability.
9. Scope will be validated during discovery phase & any additional work with be taken up as a PCR
10. IBM is not proposing any Add-ons as part of this solution
11. IBM will bill the client Monthly
12. Travel & Living will be billed to client at actuals
13. OOB Salesforce Permits Portal Application will be leveraged & no mobile specific optimizations are in scope
14. Following activities are not in IBM Scope
    1. Customer Support (Call/Chat)
    2. Paper to Digital Scanning

Solution Scope Boundaries

Permits Portal Implementation
- Delivery of a unified digital permitting portal serving citizens and businesses as a single point of entry, and supporting internal State staff for end-to-end application processing across seven agencies.
- Up to 25 user interface screens will be implemented for public and internal users.
- Solution includes approximately 130 workflow flows, 130 configuration items, 21 controlled customizations, and 31 defined integrations.
- IBM will use the Salesforce Public Sector Solutions out-of-the-box portal template with an estimated 80% configuration and 20% customization.
- The client-facing interface will use the standard out-of-the-box Salesforce UI, with limited visual modifications.

Backend Integrations
- Integration with 10 legacy systems and 3 enterprise services including payments, GIS, and document repositories.
- The State will be responsible for exposing required middleware interfaces and endpoint specifications needed for integration.
- IBM will configure integrations based on available and documented APIs.

Reporting and Dashboards
- Delivery of up to 100 standard operational reports and 15 interactive dashboards for agency leadership and public transparency.
- Approximately 80% of reporting will rely on Salesforce out-of-the-box analytics capabilities.

Change Management and Training
- Training for up to 300 State users, including 2–3 champions per agency.
- Development of up to 25 role-based training modules and job aids (approximately 30 minutes each).
- Conduct up to five train-the-trainer sessions, each one business day in length.
- The State will lead overall change management activities; IBM will provide communications support only.

Data and Content Migration
- Migration of up to 2 TB of digital data supplied by the State.
- IBM will provide the target data format and will load the data as provided by the State.
- Data cleansing, correction, enrichment, and transformation outside the target format are out of scope.

Hypercare Support
- 30-day post-go-live Hypercare period covering stabilization and issue resolution.
- 24/7 response for Priority-1 critical issues during the Hypercare window.

Application Management Services (AMS)
- Up to 12 months of AMS support, limited to the capacity funded within the contract.
- Activities include validation and verification of Salesforce seasonal release updates.
- AMS scope is limited to Level 2 and Level 3 support; Level 1 and Level 1.5 remain with the State.
- Minor or major enhancement requests are not included and will require separate change control.