SpruceID

One-Stop-Shop Permitting Portal

State of West Virginia

Proposal Prepared by: Spruce Systems, Inc. (dba SpruceID)

FedEx® Tracking

DELIVERED

Wednesday

12/3/25 at 10:16 AM

SpruceID

RFP Subject:

State of West Virginia One-Stop-Shop Permitting Program

RFI Number:

CRFP 0201 SEC2600000001

Vendor Details:

Name:
Spruce Systems, Inc. (dba SpruceID)

Address:
228 Park Avenue South, #28788
New York, NY 10003

Phone Number:
+1-917-300-9766

Fax Number:
n/a

Contact Details:

Wayne Chang
Founder and CEO
Phone: +1-917-300-9766
Email: wayne@spruceid.com

Signed,

DocuSigned by:
Wayne Chang
C4EE4516A56C49F...

CEO

11/26/2025

I. Executive Summary

The State of West Virginia has set a clear goal through W. Va. Code §5A-13-1 et seq.: to create a unified, modern One-Stop-Shop Permitting Portal that simplifies how residents, businesses, and agencies manage licenses and permits. SpruceID's proposed solution fulfills this mandate through a secure, user-friendly, and standards-based digital platform that streamlines application workflows, improves transparency, and supports long-term statewide modernization.

SpruceID is a technology partner specializing in digital transformation for state and local governments, helping agencies replace fragmented legacy systems with interoperable, resident-centered platforms. Our work powering the Utah Verifiable Digital Credentials (VDC) Initiative and the California Department of Motor Vehicles (DMV) mobile driver's license (mDL) modernization demonstrates our ability to deliver complex, multi-agency solutions that meet legislative mandates, security requirements, and usability expectations.

The proposed West Virginia One-Stop-Shop Permitting Portal includes two connected components—a Public-Facing Portal and an Agency Dashboard—built on a secure, standards-based architecture. Together, they form a single digital environment where residents can apply for, pay for, and track permits while agencies manage approvals, monitor metrics, and configure workflows independently.

Key capabilities include:

- **Smart, Adaptive Form-Filling:** Dynamic, Q&A-style applications that tailor questions based on user responses, reducing errors and improving completion rates.
- **Document Auto-Fill via OCR:** Optical character recognition extracts data from uploaded documents to auto-populate fields, saving time and ensuring accuracy.
- **Digital Wallet Integration:** Residents receive and manage their issued permits securely, with verifiable QR codes for instant validation.
- **Configurable Workflows and Real-Time Data Exchange:** Agencies can customize processes while maintaining interoperability with existing systems via standards-based APIs.
- **Security and Reliability:** Built on global security, credentialing, and compliance standards, the system ensures resilience, transparency, and data protection.

SpruceID's approach is collaborative and adaptable. The State will have full access to project dashboards, sandbox environments, and transparent service-level reporting throughout the implementation process. Training will follow a train-the-trainer model, supported by an on-demand learning portal to ensure long-term self-sufficiency. SpruceID also offers optional U.S.-based customer support (M–F, 9 AM–5 PM ET) to ensure responsive assistance throughout implementation and ongoing operations.

The result is a single, trusted digital platform that allows West Virginians to complete all permitting needs quickly and confidently, while giving agencies the tools they need to manage operations efficiently. SpruceID's solution delivers more than a technology upgrade—it establishes the foundation for a modern, interoperable digital government ecosystem that will continue to evolve and scale as new agencies join.

II. SpruceID Overview & Experience

SpruceID is a technology company that helps governments modernize legacy systems, streamline digital workflows, and improve resident access to public services through secure, standards-based platforms. Our solutions enable agencies to move away from paper-based, siloed systems and toward interoperable digital environments that support faster service delivery, stronger security, and better user experience.

SpruceID's core expertise lies in designing secure, highly usable, and interoperable digital government platforms. Our solutions have been recognized for excellence in user experience, including the Gartner Eye on Innovation Award and the success of the California DMV mobile driver's license (mDL) application, which maintains a 4.8-star rating with over 100,000 public reviews. These programs demonstrate SpruceID's ability to deliver award-winning, accessible, and resident-centered digital services at statewide scale.

Modernization and Systems Integration Experience

SpruceID's approach to modernization is pragmatic: we work with agencies to build upon existing investments rather than replace them. Our platforms and implementations are designed to integrate with legacy systems, middleware, and third-party tools using secure APIs and event-driven data exchange—allowing governments to deliver modern digital experiences without disrupting core operations.

This approach has been proven through major state-level initiatives, including:

Utah Verifiable Digital Credentials (VDC) Initiative – SpruceID partnered with the Utah Department of Government Operations (GovOps) to design and deploy a statewide platform for issuing and verifying digital permits and licenses, established under Utah Code §63A-16-110 et seq. The system enables multiple agencies—including the Departments of Natural Resources and Health—to issue secure digital credentials such as Off-Highway Vehicle Education Permits, Food Handler Permits, and Liquefied Petroleum Gas Certificates.

This project demonstrates SpruceID's ability to execute under a legislative mandate, coordinate across multiple agencies, and deliver interoperable digital infrastructure that improves transparency and service delivery statewide.

California Department of Motor Vehicles (DMV) – Digital Identity Modernization – SpruceID worked with the California DMV to support its mobile driver's license (mDL) and digital credentialing program. The engagement required deep integration with the DMV's Salesforce CRM, MuleSoft middleware, and mainframe system of record, ensuring real-time data exchange between legacy and modern systems.

Beyond technical integration, SpruceID collaborated with the DMV and federal partners—including the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS)—to conduct mDL testing at the Transportation Security Integration Facility (TSIF). This work validated acceptance of California mDLs at TSA checkpoints and helped shape broader inter-agency standards for digital identity verification.

Both initiatives demonstrate SpruceID's ability to deliver secure, standards-aligned systems in highly regulated, multi-stakeholder environments.

Commitment to Secure, Interoperable Modernization

Across all engagements, SpruceID's modernization strategy centers on three principles:

1. **Resident-Centered Design** – Every system we deliver prioritizes usability, accessibility, and transparency for the public. Whether applying for a license or tracking a permit, users interact through clear, guided experiences designed to minimize friction.

2. **Secure and Standards-Based Architecture** – Our platforms are built using NIST 800-53 Rev. 5, FIPS 140-3, and SOC 2 Type II compliant practices. Our proposed implementation supports WCAG 2.1 AA accessibility, encryption-by-default, robust logging, and role-based access control to meet or exceed state and federal cybersecurity expectations.

3. **Interoperability and Sustainability** – SpruceID's technology stack supports open standards and real-time APIs, ensuring long-term compatibility with state-managed cloud environments, identity systems, and data platforms. The result is a flexible foundation that can expand as new agencies, workflows, and programs are added over time.

SpruceID's experience directly aligns with the State of West Virginia's statutory goal to create a unified, statewide permitting platform under W. Va. Code §5A-13-1 et seq. Our prior work demonstrates the ability to:

- Modernize core systems without replacing existing agency technology;
- Deliver a single, intuitive user experience across multiple programs; and
- Meet legislative mandates for implementation timelines, accessibility, and interoperability.

SpruceID brings the technical capability, modernization experience, and collaborative approach needed to help West Virginia deliver on its vision of a secure, resident-centered One-Stop-Shop Permitting Portal that serves as a model for digital transformation across state government.

III. Proposed Solution Overview

SpruceID's proposed One-Stop-Shop Permitting Portal delivers a unified, easy-to-use digital system that simplifies how residents, businesses, and agencies manage permits and licenses across the State of West Virginia. The solution brings all permitting activities into a single platform—reducing manual steps, improving visibility, and supporting faster, more consistent service delivery.

System Overview

The proposed portal consists of two connected components that share a secure, standards-based backend:

- **Public-Facing Portal:** Residents and businesses can apply for permits, upload documents, make payments, and track progress through one account. The experience is mobile-responsive, WCAG 2.1 AA compliant, and designed for simplicity.

Applicants are guided through a Q&A-style form flow that uses smart logic to dynamically adjust questions and requirements based on user input—so no one sees unnecessary steps or forms. Uploaded documents (e.g., driver's licenses, insurance cards, prior permits) can optionally be processed with OCR-based auto-fill, extracting key data like names, dates, and addresses directly into the application fields to save time and prevent errors.

Throughout the process, users receive real-time feedback and contextual guidance—including tooltips, help text, and optional AI-powered assistance—to ensure forms are completed correctly the first time. When permits are issued, they appear automatically in a resident's digital wallet, ready to download, present, or renew.

- **Agency Dashboard:** Authorized staff can review and approve applications, manage workflows, and monitor program metrics in real time. Role-based access controls (RBAC) ensure that each user's view and permissions align with their responsibilities. Built-in analytics give administrators transparency into application volumes, processing times, and bottlenecks.

Both components will operate on a common data layer that maintains synchronization across agencies while enforcing strict security and privacy controls.

Core Capabilities

- **Unified Application and Tracking:** Applicants begin once, save progress, and complete all required permits in one place, with real-time status updates visible to both residents and staff.
- **Smart, Dynamic Forms:** The application process uses adaptive, question-driven logic that changes based on the user's responses—eliminating confusion, reducing data entry, and guiding each applicant through only the steps that apply to them.
- **Configurable Workflows:** Agencies can tailor approval steps, forms, and notifications without new development.
- **Secure Payment and Digital Wallet:** Integrated payment gateways allow residents to pay fees, track refunds, and securely store digital permits and licenses. Each credential includes a verifiable QR code or barcode that can be scanned and validated instantly.
- **Document Upload and Auto-Fill:** The system optionally includes OCR document scanning and field extraction, allowing users to upload documents (e.g., identification, certifications, or site plans) and automatically populate related form fields, dramatically reducing manual input and processing time.
- **Real-Time Data Exchange:** APIs connect to existing systems, middleware, and legacy databases, minimizing disruption to current operations.

The portal will be designed to make government interactions intuitive, transparent, and reliable. Applicants can begin an application on any device, save progress mid-process, and return later without losing data. Intelligent form guidance reduces rework, and automated prompts ensure all required documents are uploaded before submission.

Residents receive clear, proactive communication—via email or SMS—at each stage of review, while agencies gain a consolidated view of every application, document, and action taken. The result is a seamless, end-to-end experience for both applicants and administrators.

In summary, SpruceID's proposed solution provides the State of West Virginia with a secure, modern, and scalable permitting platform that enhances user experience, reduces administrative burden, and improves operational transparency across agencies.

The following sections of this proposal detail how our solution meets each of the specific functional, technical, and security requirements outlined in the RFP.

IV.Goals and Objectives

Requirement	Our Response
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.	SpruceID proposes a proven, user-centered methodology to design, develop, and deploy West Virginia's One-Stop-Shop Permitting Portal, consisting of two tightly integrated components: 1. **Public-Facing Dashboard and Citizen Portal**, where residents and businesses can apply for, track, and manage permits and licenses across agencies; and 2. **Agency Administration Dashboard**, providing configurable workflows, review tools, and performance analytics for state and local agencies. Our approach combines human-centered design, agile development, and modular engineering to ensure that both the public and agency interfaces are intuitive, accessible, and fully compliant with the statutory requirements of House Bill 2002 and Legislative Rule 148CSR25. **Phase 1 — Discovery and User Research** SpruceID will conduct structured workshops and interviews with representative users—including applicants, contractors, and agency personnel—to capture pain points and functional needs across permitting workflows. Deliverables include: • User personas and journey maps • Information architecture and navigation model • Wireframes for both public and internal dashboards • Prioritized schedule for integrating Agency permit workflows **Phase 2 — Design and Prototyping** Using insights from discovery, our design team will create high-fidelity prototypes of the Citizen Portal and Agency Dashboard. The design will emphasize:

- Simple, question-and-answer (Q&A) form completion replacing static PDFs;
- Clear visual indicators of application status, required actions, and messages;
- Unified branding consistent with the State's digital identity guidelines; and
- Embedded help and contextual guidance to reduce support requests.

Interactive prototypes will be tested with real users to validate clarity, accessibility, and overall satisfaction before development begins.

Phase 3 — Iterative Development and Integration

SpruceID's engineering team will implement the portal using our **Credible** platform as the secure backend. Key activities include, but are not limited to:

- Configuring reusable components for application intake, review, approval, and issuance;
- Connecting the portal with agency employee identity system(s);
- Developing role-based dashboards for each agency;
- Implementing APIs for integration with existing permitting databases, GIS systems, and payment gateways; and
- Establishing a unified data model for cross-agency reporting.

Each sprint will conclude with stakeholder demonstrations and acceptance testing to ensure traceability from requirements to functionality.

Phase 4 — Testing, Accessibility, and Security Validation

Comprehensive testing will cover unit, integration, user acceptance, and security assessments. The portal and dashboard sites will comply with:

- WCAG 2.1 AA accessibility standards;
- NIST 800-53-aligned security controls; and
- State privacy and data-retention policies.

Phase 5 — Launch and Continuous Improvement

SpruceID will support phased roll-outs beginning with high-impact permit types and agencies. Real-time analytics and dashboards will allow administrators to monitor throughput, identify bottlenecks, and measure performance against statutory KPIs.

Post-launch, we will establish an iterative enhancement cycle, informed by user feedback, to refine the interface, improve self-service features, and expand functionality as new agencies join the platform.

Result

The resulting One-Stop-Shop Portal will provide:

- A unified, mobile-friendly experience for citizens and businesses;
- Configurable tools for agencies to manage end-to-end workflows without

	vendor intervention; • Centralized analytics to support transparency and oversight; and • A scalable foundation to accommodate future permit types and digital services.
4.2.1.2 Vendors should describe how they would implement a flexible and secure Role-Based Access Control system.	Our proposed solution will incorporate a flexible, secure, and auditable Role-Based Access Control (RBAC) framework within the One-Stop-Shop Permitting Portal to ensure that users have access only to the data and functionality required for their roles. The model is designed to balance centralized policy enforcement with agency-level autonomy, enabling each participating entity to manage its own users while maintaining consistent statewide security standards. **Design Principles** The proposed RBAC model is guided by three core principles: 1. **Least Privilege:** Each user is assigned the minimum set of permissions necessary to perform their duties. 2. **Separation of Duties:** Administrative, review, and approval functions are clearly segmented to reduce risk and enhance accountability. 3. **Configurability and Scalability:** Roles, permissions, and hierarchies can be adjusted through administrative configuration as new agencies and permit types are added. **Architecture and Controls** The proposed RBAC system will be integrated into the Credible platform, which serves as the secure backend for the permitting portal. Key features include: • **Granular Role Definition:** The system supports multiple user roles (e.g., state administrator, agency administrator, permit reviewer, finance officer, public user), each mapped to specific workflows, data fields, and dashboards. • **Attribute-Based Extensions:** In addition to static role assignments, conditional access rules (e.g., by agency, permit type, or geographic region) may be applied via the State's SSO system to achieve fine-grained control. • **Centralized Authentication:** The solution is designed to integrate with the State's identity provider(s) using standards such as SAML 2.0 or OIDC, supporting Single Sign-On (SSO) and optional multifactor authentication (MFA). • **Delegated Administration:** Authorized agency personnel will be able to manage their own staff accounts and permissions, while statewide administrators maintain overarching visibility. • **Comprehensive Audit Logging:** All authentication events, role changes, and permission updates will be recorded in detailed audit logs that can be exported to the State's Security Information and Event Management (SIEM) system.

	Implementation Process Our proposed implementation approach includes: 1. **Requirements Definition:** During discovery, we will collaborate with the Department of Administration and agency stakeholders to document existing access models and desired governance structures. 2. **Configuration and Mapping:** Roles and permissions will be configured within the Credible platform and mapped to workflows and data elements based on agency requirements. 3. **Testing and Validation:** Role assignments and access restrictions will undergo validation through user acceptance testing (UAT), penetration testing, and security review. 4. **Ongoing Governance:** Post-launch, the RBAC model will remain fully configurable through administrative tools, allowing the State to add new roles or agencies without requiring additional vendor development. **Security Compliance** The proposed RBAC framework is designed to align with: • NIST SP 800-53 Rev. 5 (Access Control and Audit and Accountability controls); • ISO/IEC 27001 principles for information security management; and • Applicable State of West Virginia cybersecurity and identity management standards.
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.	Our proposed solution will feature a user-friendly and responsive interface designed to guide applicants through every stage of the permitting lifecycle—from initial submission through review, approval, and renewal—while providing clear visibility into progress and next steps. The interface will support both individuals and businesses, enabling users to manage multiple applications and to apply for additional permits or licenses within a unified, intuitive environment. The design approach emphasizes clarity, transparency, and accessibility. All content will be presented in plain language, supported by contextual help and visual indicators that make complex permitting processes easy to follow. Users will be able to view real-time updates on application status through a centralized dashboard that reflects milestones such as “Submitted,” “In Review,” “Pending Payment,” or “Approved.” Notifications by email, SMS, or optional push alerts will keep applicants informed of key actions required or approvals received, reducing uncertainty and minimizing the need for agency follow-up. Within the same interface, applicants will have the ability to initiate new or related applications without re-entering information. Previously submitted data and uploaded documentation will be available for reuse, supporting a “single account, multiple applications” model. This streamlined approach simplifies interactions for

	contractors, businesses, or individuals who frequently engage with multiple permitting processes. The proposed interface will employ a modern, responsive design framework to ensure usability across desktops, tablets, and mobile devices. Accessibility will be treated as a core design requirement, meeting or exceeding WCAG 2.1 AA standards through appropriate color contrast, keyboard navigation, and screen-reader compatibility. The interface will also adhere to the State's digital branding and usability guidelines to maintain a consistent public experience. Usability testing will occur iteratively throughout development. Prototypes and early releases will be evaluated with representative user groups to validate clarity, navigation, and visual design. Feedback gathered during these sessions will directly inform refinements before and after launch, ensuring that the portal remains intuitive and inclusive for all West Virginians.
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.	Our proposed solution will include an optional, embedded interactive guidance assistant that operates exclusively within a Zero-Data-Retention (ZDR) environment. No State data will be stored by external AI providers and no information will be used to train third-party models. All guidance logic is performed using on-device or ephemeral processing. The State may fully disable this feature at any time. This design ensures full compliance with the State's restrictions on cloud-based artificial intelligence and the West Virginia Office of Technology (WVOT) data-protection policies. The proposed approach combines structured guidance with light-weight AI augmentation to make the experience feel interactive and adaptive while remaining straightforward to implement and maintain. The assistant will support users in three key ways: • **Step-by-Step Guidance:** The system will present applications through a conversational, question-and-answer (Q&A) flow rather than long, static forms. Each question is contextualized based on the user's prior responses, displaying only relevant fields and requirements. • **Inline Help and Validation:** As users complete forms, the assistant will surface tooltips, help text, and short clarifying prompts (for example, "You can find this number on your business registration certificate"). Inline validation will flag missing or inconsistent entries before submission, reducing staff review time. • **Smart Prompts and Document Assistance:** Where appropriate, the system may offer document assistance using privacy-preserving, zero-retention OCR and structured prompt logic hosted entirely within the State's boundary. No uploaded documents or extracted fields are transmitted to external AI models, and the State retains full control over enabling or disabling these optional workflows. The assistant will be visible as a persistent help icon and through inline prompts within each application flow. It will not require external data storage, ensuring full compliance with State privacy and data-residency requirements. The system will log

	interactions for quality assurance but will not retain or transmit user content for model training. Over time, additional prompts or workflows can be added through administrative configuration, allowing agencies to update help content or guidance language without vendor intervention. By combining adaptive forms, contextual guidance, and optional AI-enhanced assistance, our proposed solution will provide a user experience that feels intelligent and responsive, while remaining practical to deploy within the State's timeline and infrastructure constraints.
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.	Our proposed solution will include a dynamic, transparent tracking system that provides applicants with real-time visibility into the progress of their submissions across every stage of the approval workflow. This capability will be fully embedded in the public dashboard and powered by the workflow logic and audit features of the Credible platform, allowing applicants, reviewers, and administrators to share a single source of truth regarding status and next steps. The system is designed to display each application's current position in the approval process using clear, plain-language milestones such as *Submitted*, *Under Review*, *Awaiting Documentation*, *Pending Payment*, and *Approved*. Status updates will occur automatically as reviewers complete actions or system events are logged within the underlying workflow engine. Because these updates are data-driven, applicants receive accurate, near real-time information without requiring manual intervention from agency staff. In addition to the primary status indicator, the dashboard will include contextual details such as submission date, assigned agency or reviewer, outstanding tasks, and expected response time. Applicants may also opt-in to receive notifications—via email, SMS, or push alert—whenever a status change or action item occurs. All messaging will use templated content configured by agency administrators to ensure consistency and compliance with communication policies. To maintain transparency, each application record will maintain a chronological activity log that captures completed actions, reviewer comments, and system events. This log provides both applicants and agency staff with a clear audit trail, improving accountability while reducing the need for direct status inquiries. For administrators, aggregated workflow data will feed into the internal dashboard to support performance monitoring and reporting across agencies. From a technical standpoint, the tracking system will leverage Credible's API and event-driven architecture. When a workflow transition occurs—such as a permit being assigned, reviewed, or approved—the platform will automatically publish an update that the public dashboard consumes in real time. This approach eliminates data duplication and ensures synchronization between the public and internal systems. The interface will be responsive and accessible, ensuring that all tracking features perform consistently across devices and meet WCAG 2.1 AA accessibility standards. The layout will be optimized for mobile users, presenting essential status information at a glance with expandable details for deeper insight. By integrating workflow automation, audit logging, and user-friendly visualization, our proposed solution will provide West Virginia residents and businesses with a clear, trustworthy view of their application progress. This transparency will enhance

	public confidence, reduce administrative workload, and align the permitting experience with the modern service standards envisioned under House Bill 2002.
4.2.1.6 Vendors should explain how the solution will implement a robust session management and draft-saving system for mid-process applications.	Our proposed solution will implement a robust session management and draft-saving system that allows applicants to securely pause and resume permit or license applications without losing progress. This capability is designed to improve user experience, reduce abandonment rates, and accommodate the complex, multi-step nature of government permitting processes. The proposed system will maintain session integrity through secure, token-based authentication aligned with industry standards such as OAuth 2.0 and OpenID Connect. When a user begins an application, the system will create an encrypted session identifier linked to their authenticated account. If the session becomes inactive—for example, due to time-out or network interruption—the user can securely resume their progress by reauthenticating. Session timeouts will be configurable to meet state security policies and balance usability with protection against unauthorized access. Draft-saving functionality will operate seamlessly in the background. As applicants complete sections of the application form, the system will automatically save responses in real time to prevent data loss. Saved drafts will be stored in the user's authenticated workspace within the platform, using encrypted storage and field-level validation to ensure that only complete and valid data is preserved. Where appropriate, the interface may also use local browser caching to temporarily retain unsaved input, adding an additional layer of resilience against unexpected disconnections or browser closures. Users will have full control over their drafts, with options to manually save, review saved versions, or delete incomplete submissions directly from their dashboard. Each saved draft will display its last updated timestamp and a clear indication of remaining steps or required documentation. When users return, the application will resume exactly where they left off, restoring both entered data and navigation state. For multi-agency or multi-permit workflows, draft-saving will extend across multiple forms within a single project submission. Applicants will be able to complete one section, pause, and return later to add supporting permits or additional information, ensuring a continuous and organized process even for complex applications. Session and draft data will be protected by the same encryption and access controls applied to all user data within the platform. Drafts will remain private to the applicant until formally submitted, at which point workflow automation will trigger agency review and audit logging.
4.2.1.7 Vendors should describe how the solution implements a transparent and dynamic time-tracking module within the public dashboard.	Our proposed solution will include a transparent, dynamic time-tracking module integrated directly within the public dashboard to help applicants understand the expected and actual duration of each stage in the permitting process. This feature is designed to promote accountability, set realistic expectations for residents and businesses, and align with the transparency objectives established under House Bill 2002. The time-tracking module will automatically capture timestamps from the Credible platform's workflow engine, recording each transition—such as application submission, agency assignment, review, request for information, and final approval. These timestamps will populate a user-friendly timeline displayed within the

	applicant's dashboard, showing how long the application has spent in each status and the total elapsed time since submission. To enhance usability, the interface will present time-tracking information in a visual format that includes: • **Progress Indicators:** A horizontal or vertical progress bar that highlights completed and pending stages, accompanied by descriptive labels such as *Under Review* or *Awaiting Applicant Action.* • **Estimated vs. Actual Time:** A comparison of the average processing time for similar applications versus the applicant's current progress, giving users realistic expectations for completion. • **Milestone Notifications:** Automatic alerts when an application exceeds an established timeframe, helping agencies proactively manage bottlenecks and applicants stay informed. All timing data will be drawn directly from workflow metadata, ensuring accuracy and eliminating the need for manual updates by agency staff. Agency administrators will also have access to aggregated reporting through the internal dashboard, allowing them to analyze processing times, identify delays, and monitor compliance with statutory or service-level commitments. From a technical perspective, the proposed module will leverage audit and event-logging capabilities within the Credible platform. Each workflow transition event will trigger a timestamp that is written to the application record, securely stored, and displayed through the dashboard's API layer. This approach ensures full synchronization between the internal and public views of time data and maintains an immutable record of process history for auditing purposes. The design will remain consistent with accessibility standards (WCAG 2.1 AA) and mobile responsiveness requirements, ensuring that time-tracking visualizations are legible and navigable on all devices. Where users rely on screen readers, the module will provide text-based summaries describing elapsed and expected durations for each phase.
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.	Our proposed solution includes a mobile-friendly, fully offline-capable inspection module that enables field inspectors to conduct site visits, complete checklists, capture evidence, and submit reports even when network connectivity is unavailable. This capability ensures operational continuity in rural or low-connectivity environments common across West Virginia, while maintaining the same data integrity, auditability, and security controls as online workflows. The inspection module is built as a Progressive Web Application (PWA), allowing inspectors to access assigned tasks, review permit details, and record findings directly from smartphones or tablets. When an inspector begins an assignment, all relevant data—including permit information, location details, prior submissions, and inspection criteria—is securely cached on the device for offline use. While offline, inspectors can: • Complete digital inspection forms and structured checklists; • Attach photos, geolocation metadata, timestamped notes, and evidence files;

	• Record pass/fail determinations or conditional approvals; and • Generate draft inspection summaries for later submission. All offline entries are stored in FIPS 140-3 validated, AES-256 encrypted local storage, ensuring protection against data loss or unauthorized access. Sensitive data remains tied to the inspector's authenticated session and is protected with automatic session expiration when idle. Once network connectivity is restored, the inspection module automatically queues and synchronizes all offline entries with the central system. Synchronization uses a transaction-safe, conflict-resilient process that prevents overwrites, duplication, or partial updates and ensures that each action is captured in the system's audit trail. Inspectors receive clear visual indicators of sync status (such as "Pending Upload" or "Synced Successfully"), while supervisors can monitor inspection assignments and completion rates in near real time once data is uploaded. The interface is optimized for field environments, with large touch-friendly controls, minimal text-entry requirements, and clear prompts that guide users through required steps. All features—including offline storage, synchronization, and audit logging—operate fully within the State's FedRAMP Moderate–authorized cloud boundary, consistent with WVOT security and privacy requirements. This offline-first design ensures that field inspectors can work reliably anywhere in the State while maintaining complete data integrity, security, and transparency across all inspection workflows.
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.	Our proposed solution will be fully accessible and optimized for mobile devices to ensure consistent functionality, usability, and performance for both public and agency users. The platform is designed with a mobile-first, responsive architecture, enabling all major features—including application submission, status tracking, approvals, and inspections—to operate seamlessly across smartphones, tablets, and desktop environments. The proposed design approach prioritizes accessibility and performance equally. All user interfaces, including the public dashboard and agency administrative modules, will automatically adjust to the screen size and orientation of the device in use. Form layouts, navigation menus, and data visualizations will reflow dynamically to maintain readability and ease of interaction. This ensures that residents applying for permits and inspectors conducting field operations experience the same level of usability regardless of device type or network conditions. To support mobile responsiveness, the solution will be developed using progressive web application (PWA) principles and modern frontend frameworks that optimize for lightweight performance and cross-platform compatibility. This approach enables rapid page load times, smooth navigation, and offline resiliency while avoiding the maintenance overhead of separate native mobile apps. Accessibility will be treated as a core design requirement rather than an enhancement. The platform will comply with WCAG 2.1 AA standards and relevant state accessibility guidelines, ensuring compatibility with assistive technologies

	such as screen readers, voice input, and keyboard navigation. Interactive elements—including buttons, form fields, and progress indicators—will meet touch-target and contrast ratio standards to ensure ease of use for all users. For agency staff using mobile devices, administrative dashboards and inspection modules will retain full functionality without requiring a desktop environment. Field inspectors will be able to review assigned permits, capture photos, and submit results directly from tablets, while managers can review submissions or approve workflows through secure mobile sessions with multi-factor authentication. Performance optimization will be achieved through efficient data caching, content delivery networks (CDNs), and adaptive image compression. These techniques ensure that the application remains responsive even under limited bandwidth conditions often encountered in rural areas. Background synchronization will allow users to continue working uninterrupted while data uploads occur automatically when connectivity improves.
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.	Our proposed solution will implement a flexible, user-controlled notification system that keeps residents and businesses informed of key milestones throughout the permitting process. The notification framework is designed to enhance transparency and reduce uncertainty by delivering timely updates through the user's preferred communication channel—email, mobile SMS, or both. The notification system will be integrated directly into the Credible platform's workflow engine, ensuring that messages are triggered automatically as applications move through defined stages such as submission, payment, review, approval, and renewal. Each event within the workflow will correspond to a configurable notification rule, allowing agencies to determine which events generate alerts and what content is included. At account setup, users will be prompted to select their notification preferences and may update them at any time through the account settings menu. Options will include: • **Email notifications** for detailed correspondence, status updates, and official confirmations; • **SMS notifications** for brief, time-sensitive alerts such as "Action required" or "Application approved"; and • **Combined or tiered delivery**, allowing users to receive high-priority alerts by both channels while opting for a single channel for routine updates. All messages will use pre-approved templates that ensure consistency, clarity, and compliance with state communication policies. Templates can be tailored by agency administrators without vendor intervention, allowing each department to align message content and branding with its specific operations. The notification framework will use secure integration with standard email and SMS delivery services through encrypted APIs, ensuring high deliverability while maintaining compliance with applicable privacy and anti-spam regulations. Personal contact data will be encrypted at rest and in transit, and users will retain full control over opting in or out of specific communication types. From an operational perspective, all outgoing messages and delivery confirmations will be logged within the system's audit trail. Agency staff will have visibility into

	when messages were sent, delivered, and opened, supporting both customer service and compliance reporting.
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.	Our proposed solution will include a flexible, secure, and user-friendly form and document management module that allows applicants to upload supporting materials or complete fillable digital forms as required for specific permit types. The module is designed to simplify data entry, reduce manual handling of paper-based documents, and provide agencies with consistent, structured data for efficient review and approval. The form management component will support both configurable digital forms and document upload workflows. For each permit type, agencies will be able to define custom intake forms using an administrative interface that allows the addition, removal, or modification of fields without vendor intervention. Form logic will be dynamic and conditional, ensuring that users are presented only with questions relevant to their specific situation. This adaptive approach minimizes confusion and improves data quality while reducing staff time spent on incomplete submissions. Applicants will have the ability to upload supporting documents—such as plans, certifications, or identification materials—directly through the public portal. Each upload will be scanned for file type compliance and securely stored in encrypted repositories managed under the State's designated cloud environment. Uploaded files will be associated with the relevant application record and accessible only to authorized agency staff in accordance with defined role-based access controls. The module will also support fillable PDF generation and digital signature capture, enabling agencies to replicate existing paper-based forms within an online workflow. This ensures continuity for permit types that require official document formatting or signatures while eliminating the need for physical submission. Where applicable, optical character recognition (OCR) and visual language model (VLM) tools may be integrated to extract key fields—such as name, address, or license number—from uploaded files. These tools would operate within a Zero-Data-Retention (ZDR) environment to maintain full compliance with State privacy and data protection requirements. From the agency perspective, all form and document submissions will be managed within a centralized administrative dashboard. Authorized users will be able to view, annotate, and download attachments, as well as configure document retention policies in accordance with applicable records management laws. Versioning and audit trails will ensure that any document changes or replacements are recorded for accountability and compliance. To ensure usability, the document upload and form interfaces will be designed for clarity and accessibility. The layout will feature intuitive drag-and-drop functionality, clear file size and format guidelines, and progress indicators for large uploads. The system will comply with WCAG 2.1 AA standards and perform consistently across mobile, tablet, and desktop devices.
4.2.1.12 Vendors should demonstrate strategic implementation of the tool for both agencies and public users, vendors should showcase their	Our proposed solution will be implemented through a strategic, phased approach designed to maximize adoption, minimize disruption, and ensure interoperability with West Virginia's existing permitting portals and related agency systems. The implementation strategy is informed by SpruceID's experience delivering statewide platforms that unify diverse workflows under a shared technical framework while preserving agency autonomy.

ability to seamlessly integrate with existing portals and permitting systems while enhancing functionality, accessibility, and user experience.	At its foundation, the proposed solution will use Credible, SpruceID's configurable permitting and credentialing platform, as the secure backbone for managing applications, workflows, and inter-agency data exchange. The system is designed for modular deployment and open interoperability, allowing it to coexist with current systems and progressively enhance their functionality and accessibility over time. The implementation process will begin with a discovery and integration planning phase, during which our team will collaborate with the Department of Administration and participating agencies to map existing workflows, data sources, and system interfaces. This process will identify where direct API integrations, data synchronization, or embedded portal components are most appropriate. Our proposed approach emphasizes incremental onboarding, allowing early-adopter agencies to realize value quickly while informing subsequent rollouts with lessons learned. From a technical standpoint, integration will be achieved through standards-based APIs and secure data connectors. The solution will support bidirectional exchange of application data, payment confirmations, and status updates with existing permitting systems, GIS databases, and financial management platforms. This architecture eliminates redundant data entry and enables agencies to retain their current systems of record while contributing to a unified, statewide view of permitting activity. For public users, the implementation will result in a seamless experience across systems and devices. Applicants will interact with a single, consistent interface regardless of which agency owns the underlying permit process. Embedded links or redirects from existing agency websites can route users directly into the unified permitting portal, preserving familiar digital entry points while providing an upgraded, modernized experience. For agency users, the transition will focus on interoperability and continuity. Existing permitting data can be imported or synchronized into the new platform through secure migration utilities, ensuring that staff maintain access to legacy records. The system's configurable workspace model allows each agency to manage its own workflows, forms, and reporting tools within a shared infrastructure—enhancing coordination without requiring full system replacement. Throughout implementation, SpruceID's team will prioritize user experience and accessibility as key success metrics. The platform's design system ensures that all user interfaces remain intuitive, mobile-responsive, and compliant with WCAG 2.1 AA accessibility standards. Training and knowledge-transfer sessions will be conducted with both technical and non-technical agency staff to ensure long-term self-sufficiency and smooth adoption. By combining modular integration, user-centered design, and incremental rollout, our proposed solution will provide West Virginia with a modern permitting platform that enhances functionality, accessibility, and usability across all participating agencies. This strategy ensures near-term impact through early deliverables while establishing a durable foundation for future modernization efforts statewide.
4.2.1.13 Vendors should demonstrate how their solution would provide effective data security and protection, alongside ongoing support,	Our proposed solution will be implemented with robust data security, privacy protection, and continuous maintenance practices to ensure the integrity, availability, and long-term sustainability of the One-Stop-Shop Permitting Portal. SpruceID's architecture is built to align with leading security frameworks while providing the flexibility for ongoing updates, optimization, and adaptation to the State's evolving needs.

maintenance, and adjustment of the program and dashboard to meet changing needs.	**Data Security and Protection** The proposed solution will adhere to a defense-in-depth security model, incorporating multiple layers of protection across application, network, and infrastructure levels. All data—whether at rest or in transit—will be encrypted using industry-standard protocols (AES-256 and TLS 1.2+). The system will support deployment in a state-managed cloud environment, ensuring full control over infrastructure, access, and data residency. Role-based access control (RBAC) will restrict data access to authorized users only, while audit logging will capture all administrative and user actions for compliance and monitoring. The platform is designed to integrate with the State's identity management systems using standards such as SAML 2.0 and OpenID Connect (OIDC), enabling Single Sign-On (SSO) and multifactor authentication (MFA) for enhanced protection. SpruceID follows privacy-by-design principles. No data will be shared externally or used for analytics beyond the purposes explicitly authorized by the State. Sensitive information is compartmentalized, and all personal data is subject to configurable retention policies managed by the State. Optional modules such as OCR or AI-assisted form completion will operate within Zero-Data-Retention (ZDR) environments, ensuring that no user content is stored or reused for training purposes. The platform will be continuously monitored for vulnerabilities, and software updates will be managed under a secure change-management process. Penetration testing, vulnerability scanning, and code reviews will be conducted on a regular basis to ensure alignment with NIST SP 800-53 Rev. 5 and ISO/IEC 27001 controls. **Ongoing Support and Maintenance** Our proposed support model includes both proactive maintenance and responsive technical assistance. SpruceID's team will provide a dedicated support channel for state administrators and agency personnel, offering tiered response times based on issue severity. Routine system monitoring and health checks will ensure high availability, while periodic updates will include performance improvements, feature enhancements, and security patches. Post-implementation, SpruceID will collaborate with the State to establish a governance and change-management framework. This structure will define how new features, integrations, or policy changes are prioritized, tested, and deployed. The goal is to ensure the system remains adaptable as legislation, agency workflows, and user needs evolve. Training sessions, documentation, and quarterly review meetings will be used to gather feedback from agencies and users. These inputs will inform iterative improvements to both functionality and user experience. Our agile delivery approach allows incremental updates without disrupting operations, ensuring that enhancements are deployed seamlessly and on schedule. **Customer Support Availability** SpruceID can provide live customer support as an optional add-on service. This includes access to U.S.-based customer support specialists available Monday–Friday, 9:00 AM–5:00 PM Eastern Time. Support coverage includes troubleshooting, issue triage, guidance on administrative tools, and escalations to engineering teams as needed. Additional support models, including extended-hours

	or 24/7 coverage, can be made available upon request. **Sustainability and Continuous Improvement** SpruceID's long-term commitment includes lifecycle support for the permitting platform, encompassing version upgrades, compatibility testing, and ongoing alignment with emerging cybersecurity and accessibility standards. As new agencies join or new permit types are introduced, the system can be expanded through configuration rather than redevelopment.
4.2.1.14 Vendors should demonstrate a comprehensive, flexible, and secure approach that supports interoperability, minimizes disruption, and enhances operational efficiency.	Our proposed solution will be implemented through a comprehensive, flexible, and secure architecture designed to interoperate seamlessly with existing systems, minimize operational disruption, and enhance the overall efficiency of permitting processes across the State. The approach leverages SpruceID's Credible platform—already proven in multi-agency environments—to unify data, workflows, and reporting while preserving the autonomy and continuity of agency-specific operations. **Interoperability** The proposed solution will be built on open standards and modular integration principles that allow it to function as both a standalone platform and an interoperable component within the State's broader digital ecosystem. The system will support RESTful APIs, JSON data exchange, and secure webhooks, ensuring compatibility with existing permitting databases, document repositories, GIS systems, and payment processors. Integration pathways will be tailored to each agency's technical maturity and readiness. Where modern APIs already exist, Credible will interface directly for real-time data synchronization. Where legacy systems remain in use, batch data exchange or secure file transfer mechanisms will enable ongoing interoperability without the need for costly system replacements. This standards-based approach ensures long-term flexibility and simplifies future integrations as new technologies or partner systems emerge. **Minimizing Disruption** Implementation of the solution will follow a phased, non-disruptive rollout strategy. Each agency will be onboarded through an incremental process that allows continued use of existing workflows during the transition period. Data migration, staff training, and parallel testing will be conducted to ensure a smooth cutover without interrupting permit issuance or citizen services. The platform's modular configuration also allows new features or agencies to be activated independently, limiting interdependencies that might otherwise cause delays. Administrative users will retain full control over form templates, workflows, and user roles, enabling them to adapt to procedural changes without requiring vendor engineering support. **Enhancing Operational Efficiency** Our proposed model enhances operational efficiency by automating routine administrative tasks, improving data visibility, and reducing manual coordination between agencies. Centralized dashboards and configurable analytics tools will

	give leadership teams real-time insight into permit volumes, processing timelines, and bottlenecks. This data-driven visibility enables continuous process improvement and supports evidence-based decision-making. By consolidating disparate systems into a unified permitting environment, the platform eliminates duplicate data entry, shortens review cycles, and provides a consistent user experience for both applicants and staff. Integration with existing identity management and payment infrastructure further streamlines operations and reduces maintenance overhead. **Secure and Sustainable Foundation** All interoperability features will be delivered within a secure, auditable framework that maintains compliance with State IT and cybersecurity policies. Encryption, authentication, and access control protocols will extend to all integrated systems, ensuring that data exchanged across interfaces remains protected throughout its lifecycle.
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-13-1 et seq., which mandates full implementation of the One-Stop-Shop Permitting Program by January 1, 2027.	Our proposed strategy recommends a phased, integration-first approach that achieves full compliance with W. Va. Code §5A-13-1 et seq. by January 1, 2027, while minimizing disruption to existing agency systems. This approach prioritizes interoperability, continuity, and rapid value delivery—enabling the State to modernize its permitting infrastructure without sacrificing current functionality or service continuity. **Integration vs. Replacement Strategy** Our proposed solution is designed to integrate with existing agency permitting systems wherever practical, allowing each agency to participate in the One-Stop-Shop program at its current level of technical maturity. Rather than pursuing wholesale system replacement, our model supports progressive integration through secure APIs, data synchronization, and phased onboarding. This strategy minimizes risk, preserves prior technology investments, and ensures that agencies can continue operating efficiently during the transition. Each participating agency will be evaluated across three readiness tiers: 1. **Direct Integration:** For agencies with modern, API-enabled systems, the One-Stop-Shop platform will connect directly to exchange application, payment, and status data in real time. 2. **Hybrid Coexistence:** For agencies with partially modernized systems, the platform will synchronize essential data while maintaining certain legacy processes internally. 3. **Targeted Replacement:** For agencies with outdated systems that lack integration capabilities, replacement can occur gradually after initial onboarding, leveraging the Credible platform as the unified permitting backbone. This integration-first approach enables rapid implementation while providing a clear path toward long-term consolidation under a common permitting framework. **Implementation Timeline**

	or 24/7 coverage, can be made available upon request. **Sustainability and Continuous Improvement** SpruceID's long-term commitment includes lifecycle support for the permitting platform, encompassing version upgrades, compatibility testing, and ongoing alignment with emerging cybersecurity and accessibility standards. As new agencies join or new permit types are introduced, the system can be expanded through configuration rather than redevelopment.
4.2.1.14 Vendors should demonstrate a comprehensive, flexible, and secure approach that supports interoperability, minimizes disruption, and enhances operational efficiency.	Our proposed solution will be implemented through a comprehensive, flexible, and secure architecture designed to interoperate seamlessly with existing systems, minimize operational disruption, and enhance the overall efficiency of permitting processes across the State. The approach leverages SpruceID's Credible platform—already proven in multi-agency environments—to unify data, workflows, and reporting while preserving the autonomy and continuity of agency-specific operations. **Interoperability** The proposed solution will be built on open standards and modular integration principles that allow it to function as both a standalone platform and an interoperable component within the State's broader digital ecosystem. The system will support RESTful APIs, JSON data exchange, and secure webhooks, ensuring compatibility with existing permitting databases, document repositories, GIS systems, and payment processors. Integration pathways will be tailored to each agency's technical maturity and readiness. Where modern APIs already exist, Credible will interface directly for real-time data synchronization. Where legacy systems remain in use, batch data exchange or secure file transfer mechanisms will enable ongoing interoperability without the need for costly system replacements. This standards-based approach ensures long-term flexibility and simplifies future integrations as new technologies or partner systems emerge. **Minimizing Disruption** Implementation of the solution will follow a phased, non-disruptive rollout strategy. Each agency will be onboarded through an incremental process that allows continued use of existing workflows during the transition period. Data migration, staff training, and parallel testing will be conducted to ensure a smooth cutover without interrupting permit issuance or citizen services. The platform's modular configuration also allows new features or agencies to be activated independently, limiting interdependencies that might otherwise cause delays. Administrative users will retain full control over form templates, workflows, and user roles, enabling them to adapt to procedural changes without requiring vendor engineering support. **Enhancing Operational Efficiency** Our proposed model enhances operational efficiency by automating routine administrative tasks, improving data visibility, and reducing manual coordination between agencies. Centralized dashboards and configurable analytics tools will

	give leadership teams real-time insight into permit volumes, processing timelines, and bottlenecks. This data-driven visibility enables continuous process improvement and supports evidence-based decision-making. By consolidating disparate systems into a unified permitting environment, the platform eliminates duplicate data entry, shortens review cycles, and provides a consistent user experience for both applicants and staff. Integration with existing identity management and payment infrastructure further streamlines operations and reduces maintenance overhead. **Secure and Sustainable Foundation** All interoperability features will be delivered within a secure, auditable framework that maintains compliance with State IT and cybersecurity policies. Encryption, authentication, and access control protocols will extend to all integrated systems, ensuring that data exchanged across interfaces remains protected throughout its lifecycle.
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-13-1 et seq., which mandates full implementation of the One-Stop-Shop Permitting Program by January 1, 2027.	Our proposed strategy recommends a phased, integration-first approach that achieves full compliance with W. Va. Code §5A-13-1 et seq. by January 1, 2027, while minimizing disruption to existing agency systems. This approach prioritizes interoperability, continuity, and rapid value delivery—enabling the State to modernize its permitting infrastructure without sacrificing current functionality or service continuity. **Integration vs. Replacement Strategy** Our proposed solution is designed to integrate with existing agency permitting systems wherever practical, allowing each agency to participate in the One-Stop-Shop program at its current level of technical maturity. Rather than pursuing wholesale system replacement, our model supports progressive integration through secure APIs, data synchronization, and phased onboarding. This strategy minimizes risk, preserves prior technology investments, and ensures that agencies can continue operating efficiently during the transition. Each participating agency will be evaluated across three readiness tiers: 1. **Direct Integration:** For agencies with modern, API-enabled systems, the One-Stop-Shop platform will connect directly to exchange application, payment, and status data in real time. 2. **Hybrid Coexistence:** For agencies with partially modernized systems, the platform will synchronize essential data while maintaining certain legacy processes internally. 3. **Targeted Replacement:** For agencies with outdated systems that lack integration capabilities, replacement can occur gradually after initial onboarding, leveraging the Credible platform as the unified permitting backbone. This integration-first approach enables rapid implementation while providing a clear path toward long-term consolidation under a common permitting framework. **Implementation Timeline**

	Our proposed timeline follows the same five-phase structure outlined in Section 4.2.1.1, ensuring alignment across all components of the project lifecycle. Each phase builds on the previous one, leading to a statewide launch before the statutory deadline: • **Phase 1 – Discovery and User Research (Q1–Q2 2025):** Conduct stakeholder workshops, document existing systems and workflows, and define integration priorities and agency readiness tiers. • **Phase 2 – Design and Prototyping (Q2–Q3 2025):** Develop user interface mockups, data models, and dashboard prototypes reflecting agency and public user needs. • **Phase 3 – Iterative Development and Integration (Q3 2025–Q3 2026):** Configure the Credible platform, build integrations with priority agency systems, and develop public and internal dashboards through agile sprints. • **Phase 4 – Testing, Accessibility, and Training (Q3–Q4 2026):** Conduct comprehensive testing—including functional, accessibility, and security reviews—alongside staff training and documentation delivery. • **Phase 5 – Launch and Continuous Improvement (Q4 2026–Q1 2027):** Deploy the statewide public dashboard and complete phased agency onboarding to ensure full functionality by January 1, 2027, in accordance with statutory requirements. **Long-Term Sustainability** Post-implementation, SpruceID will continue to provide ongoing support, system monitoring, and feature enhancements to accommodate additional agencies and evolving policy needs. The platform's modular architecture allows future integrations, interface updates, and workflow changes to be implemented through configuration rather than redevelopment—ensuring that the solution remains secure, scalable, and adaptable over time. By following a phased integration strategy and maintaining a schedule aligned with statutory deadlines, our proposed approach ensures that the State of West Virginia achieves a fully operational, interoperable One-Stop-Shop Permitting Portal by January 1, 2027, while building a sustainable foundation for continued digital transformation.
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.	Our proposed solution will include a structured, scalable Train-the-Trainer program designed to build lasting in-house expertise within the State and its participating agencies. The goal of this model is to ensure that key agency personnel become confident, self-sufficient subject-matter experts who can effectively train and support their peers long after the initial implementation phase. **Program Structure and Objectives** The proposed training program will be delivered in three progressive tiers: 1. **Core Platform Orientation:** Introduces agency trainers to the Credible platform's interface, workflows, and administrative tools.

2. **Applied Skills Workshops:** Provides hands-on exercises focused on daily operational tasks—such as creating workflows, managing forms, reviewing submissions, and generating reports.

3. **Instructional Delivery and Coaching:** Equips designated trainers with facilitation techniques, standardized training materials, and support resources to conduct internal training sessions confidently.

This tiered structure allows the training to scale across agencies with varying levels of technical familiarity and ensures that knowledge is embedded institutionally, not vendor-dependent.

Training Materials and Resources

Our proposed solution will provide a comprehensive suite of reusable materials, including:

- Step-by-step user guides and quick-reference cards tailored to agency roles;
- Recorded video modules and slide decks for asynchronous learning;
- Scenario-based exercises using test data to simulate real permitting workflows; and
- A shared knowledge base and help-center content accessible to all trainers and administrators.

All materials will be developed collaboratively with agency input to reflect actual use cases, ensuring practical relevance and alignment with State policies and terminology.

Delivery Methodology

Training will be delivered using a blended learning model, combining virtual and in-person sessions for flexibility and accessibility. Early training sessions will be led jointly by SpruceID's implementation team and designated agency representatives. As the program progresses, agency trainers will gradually assume the lead, supported by SpruceID staff to reinforce confidence and consistency.

Each session will include interactive demonstrations, guided exercises, and Q&A segments to reinforce knowledge retention. Participants will have access to sandbox environments that mirror production systems, allowing them to experiment safely with real workflows before teaching others.

Sustainability and Ongoing Support

Following initial rollout, SpruceID will maintain engagement through refresher sessions, updated materials, and an ongoing trainer community of practice. This network will enable trainers across agencies to share best practices, troubleshoot issues collaboratively, and remain aligned as new features or modules are introduced.

Performance of the Train-the-Trainer model will be evaluated through participant feedback, training assessments, and post-training confidence surveys. Continuous improvement will ensure that materials and delivery methods evolve alongside

	system enhancements and agency needs.
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.	Our proposed solution will include a comprehensive, on-demand learning platform designed to support both agency users and public constituents after implementation. The platform will deliver accessible, self-paced training resources that reinforce ongoing adoption, minimize support requests, and ensure that users at every technical skill level can confidently engage with the One-Stop-Shop Permitting Portal. **Design and Accessibility** The learning platform will be hosted as a web-based, mobile-responsive portal accessible from the same dashboard environment as the permitting system. It will comply with WCAG 2.1 AA accessibility standards to ensure equal access for all users, including those using assistive technologies. The interface will provide intuitive navigation, search functionality, and modular learning paths tailored to different audiences—such as applicants, agency reviewers, and administrators. Each training module will be short, task-oriented, and focused on specific system functions or workflows. This approach allows users to learn at their own pace and return to individual modules as needed, rather than progressing through a linear course sequence. **Learning Content and Structure** The on-demand learning environment will feature a mix of interactive and multimedia materials, including: • Step-by-step video tutorials demonstrating core system functions; • Interactive simulations that mirror real permitting workflows; • Downloadable guides, checklists, and quick-start resources; and • Knowledge articles and FAQs linked directly from relevant screens within the application. For agency staff, dedicated modules will cover administrative tools, reporting dashboards, and workflow configuration, while public users will have access to focused tutorials on account setup, application submission, document upload, and status tracking. **Integration with the Train-the-Trainer Program** The self-paced platform will complement the Train-the-Trainer model described in Section 4.2.1.16 by serving as a shared knowledge repository that trainers can use to reinforce in-person and virtual instruction. Materials developed during implementation—such as recorded training sessions and role-specific exercises—will be uploaded into the learning portal for ongoing reference. This ensures continuity between live training and self-guided learning, while maintaining consistent messaging and procedures across agencies. **Maintenance and Continuous Improvement** SpruceID will maintain and update the learning platform as part of its ongoing support and maintenance program. New content will be added when system

	enhancements, policy changes, or new permit types are introduced. Feedback mechanisms within the platform—such as satisfaction surveys and usage analytics—will inform continuous improvement, ensuring that training materials remain relevant, effective, and aligned with user needs.
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.	Our proposed solution will be fully compatible and interoperable with the State's existing productivity ecosystem, including Google Workspace and Microsoft 365 products used for email, calendaring, meetings, and document collaboration. This compatibility is central to our design philosophy of minimizing adoption barriers, leveraging existing enterprise tools, and ensuring that agency users can work seamlessly within familiar environments. The proposed platform's open, standards-based architecture allows integration with both Google and Microsoft environments through secure APIs, SSO configurations, and data exchange protocols. Specifically, the solution will support: • **Single Sign-On (SSO) Integration:** If applicable, the system will authenticate users through the State's existing identity providers, including Microsoft Azure Active Directory (AAD) and Google Identity, using SAML 2.0 and OpenID Connect (OIDC) standards. This ensures that staff can access the permitting dashboard with the same credentials they already use for State email and productivity applications. • **Email Notifications and Calendar Integration:** Workflow-driven notifications and scheduling events—such as inspection appointments, permit renewal reminders, or application follow-up meetings—can be synchronized with users' Microsoft Outlook or Google Calendar. Notifications will use standard email delivery protocols (SMTP and API-based mail services) to ensure deliverability across both platforms without additional configuration. • **Document and File Interoperability:** Uploaded documents and generated reports can be exported, viewed, or shared in formats natively compatible with Microsoft Office (e.g., .docx, .xlsx, .pdf) and Google Workspace applications (e.g., Docs, Sheets). The solution can optionally link to shared cloud storage environments, enabling agencies to archive or collaborate on files through existing Drive or SharePoint permissions models. • **Meeting and Collaboration Tools:** For inspection scheduling, training, or inter-agency coordination, system-generated calendar events will include standard meeting links compatible with Google Meet and Microsoft Teams. This enables agency staff to launch virtual meetings directly from workflow records or notification emails without switching platforms. • **Secure Integration and Policy Compliance:** All interoperability features will adhere to the State's IT security and data retention policies. Integrations with Google and Microsoft APIs will use encrypted connections, token-based authentication, and scope-limited permissions to prevent unauthorized data access or sharing.
4.2.1.19 Vendors should explain how the solution can be adjusted to meet the growing and changing needs of the State. The	Our proposed solution is designed to adapt and scale seamlessly as the State of West Virginia's permitting environment evolves. The platform's modular, configurable architecture ensures that new agencies, permit types, and technical requirements can be incorporated incrementally—without disrupting existing

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.	operations or requiring major redevelopment. This approach provides a sustainable path for the One-Stop-Shop Permitting Program to expand in alignment with the State's long-term modernization and interoperability goals. **Flexible Multi-Agency Framework** The proposed solution will operate on SpruceID's **Credible** platform, which supports a multi-agency model through isolated workspaces and configurable administrative tools. Each agency can define its own workflows, forms, roles, and permissions within a shared infrastructure, maintaining autonomy while contributing to a unified statewide permitting ecosystem. When new agencies choose to participate, onboarding can occur through configuration rather than new code deployment. Administrative users can create new agency workspaces, define permit categories, and establish approval processes using existing low-code interfaces. This model allows expansion at any pace the State determines, minimizing cost and technical complexity. **Technical Scalability and Performance** The underlying platform is cloud-native and horizontally scalable, capable of supporting increased transaction volumes, additional datasets, and concurrent users as adoption grows. Core components—such as the workflow engine, API layer, and reporting services—can be independently scaled or extended to maintain performance and reliability as demand increases. SpruceID's architecture supports dynamic resource allocation, load balancing, and elastic storage, ensuring the system performs consistently during peak permitting cycles or when new agencies are onboarded. The modular structure also enables feature expansion—such as analytics dashboards or new integration endpoints—without requiring downtime or system reinstallation. **Evolving with the State's Needs** Our proposed solution is intentionally future-ready, allowing the State to adjust workflows, policies, and integrations as statutes, regulations, and agency responsibilities evolve. Through configurable tools, administrators will be able to modify data collection fields, document requirements, and process logic without vendor intervention. The system's adherence to open standards (RESTful APIs, JSON, and secure authentication protocols) ensures interoperability with new technologies and partner systems. As West Virginia's digital ecosystem matures, the permitting platform can integrate with evolving state and federal systems—such as identity management, payment gateways, and data analytics platforms—while maintaining full compliance with privacy and cybersecurity requirements. **Sustainable Growth and Continuous Improvement** SpruceID will support the State through an ongoing governance and improvement process that includes regular roadmap reviews, feature updates, and performance optimization. As additional agencies join, the implementation process will be repeatable, leveraging existing configuration templates, training materials, and onboarding playbooks to maintain consistency and accelerate delivery. By combining a scalable technical foundation with flexible configuration and a commitment to continuous improvement, our proposed solution will enable the State of West Virginia to expand participation and functionality over time while

	• **Integrated Payment and Digital Wallet:** Support for permit fee payments, refunds, and issuance of verifiable digital credentials through a secure wallet interface. • **Real-Time Status Tracking:** Transparent dashboards showing each application's progress through review and approval stages. • **Accessibility and Mobile Optimization:** Full compliance with WCAG 2.1 AA accessibility standards and responsive design for smartphones and tablets. The system will be deployed in a state-managed cloud environment to ensure security, data sovereignty, and compliance with West Virginia's IT and cybersecurity policies. Built on open standards and flexible APIs, the solution will interoperate with existing agency systems while laying the foundation for long-term modernization. By combining modern technology with user-centered design, our proposed approach will enable the State of West Virginia to deliver a fully integrated, citizen-centric One-Stop-Shop Permitting Portal that enhances efficiency, transparency, and accessibility for all stakeholders.
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.	Our proposed solution will be delivered using a structured, transparent, and collaborative implementation methodology that ensures timely delivery, continuous stakeholder engagement, and rigorous quality assurance throughout the lifecycle of the One-Stop-Shop Permitting Portal. The approach balances agile flexibility with disciplined project governance—ensuring measurable progress at each milestone and full alignment with the State's objectives and statutory deadlines. **Structured and Phased Delivery** The implementation will follow a five-phase agile framework—Discovery and User Research, Design and Prototyping, Iterative Development and Integration, Testing and Training, and Launch and Continuous Improvement. Each phase will culminate in tangible deliverables and review checkpoints with the State to validate progress and incorporate feedback before advancing. Work will be organized into short development sprints, typically two to three weeks in duration, with sprint reviews and retrospectives at the end of each cycle. This iterative cadence promotes adaptability, allowing requirements to evolve naturally as user testing and agency feedback inform refinements. **Transparency and Collaboration** Transparency and collaboration will be embedded at every stage. SpruceID will maintain shared project dashboards accessible to State project leads, showing current sprint status, upcoming deliverables, and identified risks or dependencies. Weekly project meetings will provide structured touchpoints for discussing progress, upcoming priorities, and decisions requiring State input. Our team will coordinate closely with agency subject-matter experts to document business rules, map existing processes, and validate each workflow prior to implementation. This collaborative process ensures that agency needs are fully reflected in the final system configuration while minimizing rework.

	Quality Assurance and Risk Management Quality assurance will be integrated into each phase of the project rather than treated as a final step. Our proposed solution includes: • **Automated and Manual Testing:** Unit, integration, and user acceptance testing (UAT) conducted during every sprint. • **Accessibility and Security Validation:** Regular reviews to confirm compliance with WCAG 2.1 AA accessibility standards and applicable State cybersecurity requirements. • **Performance Monitoring:** Load testing and optimization to ensure scalability and reliability at launch. • **Defect Tracking and Resolution:** All issues logged and prioritized in a shared tracking system for full visibility and traceability. A formal change management process will govern any scope or configuration adjustments, ensuring that all modifications are reviewed, approved, and documented before implementation. **Commitment to Timely, Quality Delivery** SpruceID's methodology emphasizes early delivery of functional components, continuous engagement with end users, and proactive quality controls. This approach minimizes risk, accelerates adoption, and ensures that the system delivered is both technically sound and operationally effective. By combining agile development practices, clear communication protocols, and comprehensive quality assurance, our proposed solution will ensure the timely, transparent, and high-quality delivery of the One-Stop-Shop Permitting Portal—fully aligned with the State's schedule, expectations, and strategic modernization goals.
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.	SpruceID fully agrees to and will meet or exceed all data security requirements established by the West Virginia Office of Technology (WVOT) for the entirety of this project. This commitment applies across every project phase—including discovery, information gathering, design, development, testing, deployment, and post-implementation support. **Comprehensive Security Commitment** Our proposed solution will be implemented within a secure, state-managed cloud or approved hosting environment, consistent with WVOT standards and policies. All activities will align with applicable State and Federal requirements, including but not limited to: • West Virginia Office of Technology Information Security Policies and Procedures; • National Institute of Standards and Technology (NIST) Special Publications 800-53 Rev. 5 and 800-63 for access control, system integrity, and identity assurance; and • ISO/IEC 27001 principles for information security management.

	SpruceID will work closely with WVOT to complete all required security design reviews, architecture assessments, and documentation submissions prior to system deployment. All system components will be reviewed and approved through the State's established processes for cybersecurity and risk management. **Security Practices Across the Lifecycle** From the earliest project stages, all personnel involved in discovery and development will adhere to WVOT's security and data-handling policies. Sensitive information gathered during planning and stakeholder interviews will be encrypted in transit and at rest, accessible only to authorized team members located within the United States (as confirmed in Section 4.2.1.24). During development and testing, SpruceID will implement least-privilege access controls, code scanning, and vulnerability management to prevent unauthorized access or data exposure. Prior to go-live, a comprehensive security review—including penetration testing and verification of encryption, logging, and authentication mechanisms—will be completed in coordination with WVOT representatives. **Ongoing Compliance and Oversight** Throughout operations, SpruceID will support WVOT in conducting periodic audits, compliance reviews, and incident-response exercises. Any identified risks or vulnerabilities will be documented, remediated, and reported in accordance with WVOT protocols and timelines. By maintaining full adherence to WVOT's security requirements across all project stages, SpruceID ensures that the One-Stop-Shop Permitting Portal will be developed, implemented, and maintained within a secure, compliant, and continuously monitored environment—protecting the State's data and the privacy of all West Virginia residents.
4.2.2.4 Vendor's proposed solution must meet FedRAMP requirements.	SpruceID affirms that the proposed solution will fully meet all applicable FedRAMP requirements, both at the infrastructure and application levels. This includes deployment within a FedRAMP-authorized cloud environment and full alignment of the permitting platform itself with the FedRAMP Moderate baseline security controls derived from NIST SP 800-53 Rev. 5. **FedRAMP-Authorized Hosting and Architecture** The One-Stop-Shop Permitting Portal will be deployed within a FedRAMP Moderate-authorized cloud environment such as AWS GovCloud (US) or Microsoft Azure Government, both of which maintain active authorizations and continuous monitoring under FedRAMP. All production, staging, and backup environments will reside entirely within this secure boundary. **Application-Level FedRAMP Compliance** Beyond hosting, the application layer of the proposed solution will be implemented, configured, and documented in full accordance with FedRAMP requirements. SpruceID will map all system and operational controls—covering access control, audit logging, encryption, configuration management, incident response, and

	continuous monitoring—to the FedRAMP Moderate control baseline. Key compliance features include: • Encryption of all data in transit (TLS 1.2+) and at rest (AES-256); • Role-Based Access Control (RBAC) with least-privilege enforcement and multifactor authentication; • Continuous monitoring, vulnerability management, and automated patching; • Comprehensive audit logging and centralized event retention; and • Annual independent security assessments consistent with FedRAMP ATO requirements. SpruceID will prepare and maintain all required security documentation—including the System Security Plan (SSP), Plan of Action and Milestones (POA&M), and Continuous Monitoring Plan—to demonstrate full alignment with FedRAMP controls and facilitate review by the West Virginia Office of Technology (WVOT). **Ongoing Compliance and Verification** Throughout the project lifecycle, SpruceID will ensure that any updates, new modules, or integrations continue to meet FedRAMP requirements. Quarterly security reviews and continuous-monitoring reports will verify control effectiveness and document remediation of any findings. No components or communications will rely on services outside FedRAMP-authorized boundaries or U.S. jurisdictions. By ensuring that both the hosting environment and the permitting solution itself comply with the full set of FedRAMP Moderate security controls, SpruceID provides the State of West Virginia with a permitting platform that is secure, auditable, and demonstrably compliant with federal and State cybersecurity standards.
4.2.2.5 Vendor must ensure all state Data is encrypted at rest and during transit. Encryption must meet FIPS 140-3 standard.	SpruceID affirms that all State of West Virginia data will be encrypted both at rest and in transit throughout the entirety of the system architecture, in strict compliance with the Federal Information Processing Standard (FIPS) 140-3 requirements. This commitment applies to all environments—development, testing, production, and backup—and includes all data storage, transmission, and integration points associated with the One-Stop-Shop Permitting Portal. **Encryption at Rest** All stored data, including databases, file repositories, backups, and document attachments, will be encrypted using FIPS 140-3 validated cryptographic modules. The system will use Advanced Encryption Standard (AES) with a 256-bit key length for all persistent storage. Keys will be managed through a secure key management service (KMS) integrated with the hosting provider's FedRAMP-authorized environment (e.g., AWS GovCloud Key Management Service or Azure Government Key Vault). Access to encryption keys will be restricted through role-based permissions, audit logging, and separation of duties to ensure that only authorized State or SpruceID security administrators can manage or rotate keys. Automated key rotation policies

	will be configured in accordance with State and federal security standards. **Encryption in Transit** All data transmitted between client devices, application servers, APIs, and integrated systems will be encrypted using Transport Layer Security (TLS) 1.2 or higher, implemented with FIPS 140-3 validated cryptographic libraries. This includes all inbound and outbound communications—whether between end users and the public portal, inter-agency systems, or third-party integrations. The solution will enforce HTTPS-only communication, secure session management, and strong cipher suites consistent with current NIST and FedRAMP Moderate baselines. External API integrations will require mutual TLS (mTLS) or token-based authentication to prevent unauthorized interception or data leakage. **Validation and Continuous Compliance** SpruceID will document and maintain evidence of FIPS 140-3 compliance as part of the system's overall security package. Regular vulnerability assessments and configuration audits will verify that encryption controls remain properly implemented and aligned with State cybersecurity policies and NIST SP 800-53 Rev. 5 control families (SC-12, SC-13, and SC-28). By ensuring that all data—both in transit and at rest—is protected with FIPS 140-3 validated encryption, SpruceID's proposed solution provides the State of West Virginia with a secure, compliant, and resilient data protection framework that meets the highest federal and State security standards.
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.	SpruceID acknowledges that it is responsible for ensuring any subcontractors utilized in this project are identified and reported to the West Virginia Office of Technology and that such subcontractors, if applicable, always maintain compliance with the State's data security requirements. SpruceID further acknowledges that it may 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	SpruceID confirms that all security controls implemented within the proposed solution will be fully in accordance with the NIST Special Publication 800-53, Revision 5, security and privacy control framework. These controls address access control, audit and accountability, incident response, system integrity, configuration management, and continuous monitoring, consistent with federal and State cybersecurity standards.

	SpruceID will provide the full NIST 800-53 Rev. 5 security documentation package required by WVOT, including the System Security Plan (SSP), Information System Contingency Plan (ISCP), Incident Response Plan (IRP), Continuous Monitoring Strategy, Configuration Management Plan, POA&M, and quarterly vulnerability scan results. Annual independent penetration testing will be conducted and delivered to WVOT. All artifacts will remain current throughout the contract term and updated upon major system changes.
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.	SpruceID's proposed solution will operate under a proactive, transparent, and standards-based security program designed to ensure system integrity, maintain compliance with State cybersecurity expectations, and provide continuous visibility into the system's security posture. **Security Program and Governance** Our security framework aligns with NIST SP 800-53 Rev. 5, FedRAMP Moderate, and ISO/IEC 27001 standards, incorporating defense-in-depth principles and continuous monitoring across infrastructure, application, and operational layers. Security controls include strict access management, audit logging, encryption, configuration hardening, and incident response procedures consistent with the West Virginia Office of Technology's policies. SpruceID maintains dedicated security and compliance personnel responsible for monitoring, reporting, and remediating potential vulnerabilities. All activities are documented, reviewed, and auditable to ensure accountability and traceability throughout the project lifecycle. **Vulnerability Scanning and Testing** The solution will include routine vulnerability scanning, penetration testing, and continuous monitoring to identify and mitigate potential risks before they impact operations. Vulnerability assessments will be performed using industry-recognized tools and methodologies covering both application and infrastructure layers. • **Frequency:** Scans will be conducted at regular intervals (at least quarterly) and following any major updates, configuration changes, or deployments. • **Reporting:** Detailed vulnerability and remediation reports will be delivered to the West Virginia Office of Technology (WVOT) on a routine schedule and immediately upon request. • **Remediation:** Identified vulnerabilities will be triaged by severity and addressed according to defined timelines aligned with WVOT security policies and NIST risk management guidance. **Transparency and Continuous Improvement** SpruceID will maintain transparent communication and collaboration with WVOT throughout implementation and operations. The State will have access to summaries of recent assessments, patching activity, and corrective action status. Security metrics and performance indicators will be included in quarterly reports to demonstrate ongoing compliance and continuous improvement.

	By integrating a proactive security posture, regular vulnerability testing, and open communication with WVOT, SpruceID's proposed solution will ensure the integrity, resilience, and trustworthiness of the One-Stop-Shop Permitting Portal while meeting and exceeding the State's cybersecurity expectations.
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.	SpruceID is committed to timely identification, prioritization, and remediation of all security vulnerabilities in accordance with industry best practices, federal guidance, and the State of West Virginia's cybersecurity expectations. Our vulnerability management program is based on the NIST SP 800-40 Revision 4 and NIST SP 800-53 Rev. 5 control frameworks, ensuring that all findings are addressed within defined, measurable timeframes. **Remediation Timeframes** SpruceID commits to the following maximum remediation windows, consistent with State and federal standards: • **Critical Vulnerabilities (CVSS 9.0–10.0):** Addressed and remediated within 15 calendar days of identification or notification. • **High Vulnerabilities (CVSS 7.0–8.9):** Addressed and remediated within 30 calendar days. • **Medium Vulnerabilities (CVSS 4.0–6.9):** Addressed and remediated within 60 calendar days. • **Low Vulnerabilities (CVSS 0.1–3.9):** Addressed and remediated within 90 calendar days or incorporated into the next planned maintenance cycle. These timelines align with the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring Strategy Guide and can be further refined in coordination with the West Virginia Office of Technology (WVOT) to meet any specific State-mandated response requirements. **Monitoring and Reporting** All vulnerabilities will be tracked within SpruceID's secure issue management system, with full lifecycle documentation from detection through remediation and verification. Quarterly vulnerability management reports—and ad hoc reports upon WVOT request—will summarize findings, remediation actions, and closure dates. SpruceID's security operations team will continuously monitor for new threats and advisories and will apply emergency patches or mitigations immediately when vulnerabilities present an active exploitation risk. By adhering to these clearly defined and auditable remediation timelines, SpruceID ensures that the One-Stop-Shop Permitting Portal remains secure, compliant, and resilient in accordance with industry best practices and State cybersecurity expectations.
4.2.2.10 The vendor must implement a resilient, secure, and verifiable strategy that ensures	SpruceID's proposed solution will include a resilient, secure, and verifiable business continuity and disaster recovery (BC/DR) strategy that ensures uninterrupted operation, data integrity, and rapid restoration of services in accordance with the State of West Virginia's expectations and the established Service Level Agreement (SLA). This strategy is designed to protect the availability and integrity of critical

	By integrating a proactive security posture, regular vulnerability testing, and open communication with WVOT, SpruceID's proposed solution will ensure the integrity, resilience, and trustworthiness of the One-Stop-Shop Permitting Portal while meeting and exceeding the State's cybersecurity expectations.
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.	SpruceID is committed to timely identification, prioritization, and remediation of all security vulnerabilities in accordance with industry best practices, federal guidance, and the State of West Virginia's cybersecurity expectations. Our vulnerability management program is based on the NIST SP 800-40 Revision 4 and NIST SP 800-53 Rev. 5 control frameworks, ensuring that all findings are addressed within defined, measurable timeframes. **Remediation Timeframes** SpruceID commits to the following maximum remediation windows, consistent with State and federal standards: • **Critical Vulnerabilities (CVSS 9.0–10.0):** Addressed and remediated within 15 calendar days of identification or notification. • **High Vulnerabilities (CVSS 7.0–8.9):** Addressed and remediated within 30 calendar days. • **Medium Vulnerabilities (CVSS 4.0–6.9):** Addressed and remediated within 60 calendar days. • **Low Vulnerabilities (CVSS 0.1–3.9):** Addressed and remediated within 90 calendar days or incorporated into the next planned maintenance cycle. These timelines align with the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring Strategy Guide and can be further refined in coordination with the West Virginia Office of Technology (WVOT) to meet any specific State-mandated response requirements. **Monitoring and Reporting** All vulnerabilities will be tracked within SpruceID's secure issue management system, with full lifecycle documentation from detection through remediation and verification. Quarterly vulnerability management reports—and ad hoc reports upon WVOT request—will summarize findings, remediation actions, and closure dates. SpruceID's security operations team will continuously monitor for new threats and advisories and will apply emergency patches or mitigations immediately when vulnerabilities present an active exploitation risk. By adhering to these clearly defined and auditable remediation timelines, SpruceID ensures that the One-Stop-Shop Permitting Portal remains secure, compliant, and resilient in accordance with industry best practices and State cybersecurity expectations.
4.2.2.10 The vendor must implement a resilient, secure, and verifiable strategy that ensures	SpruceID's proposed solution will include a resilient, secure, and verifiable business continuity and disaster recovery (BC/DR) strategy that ensures uninterrupted operation, data integrity, and rapid restoration of services in accordance with the State of West Virginia's expectations and the established Service Level Agreement (SLA). This strategy is designed to protect the availability and integrity of critical

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.	systems and data across all stages of the One-Stop-Shop Permitting Portal's lifecycle. **Business Continuity and System Resilience** The system architecture will be hosted within a FedRAMP-authorized, multi-availability-zone cloud environment to ensure continuous availability and fault tolerance. Redundant infrastructure—including load-balanced application servers, replicated databases, and distributed storage—will mitigate the impact of component failure or regional outages. All platform components will be continuously monitored for performance and health metrics. Automated failover mechanisms will route traffic to secondary nodes in the event of service degradation or failure, maintaining system availability in accordance with SLA uptime commitments. **Data Integrity and Backup Management** Data integrity will be protected through real-time replication and scheduled backups at multiple secure locations within the United States. Backups will be encrypted using FIPS 140-3 validated algorithms (AES-256) and stored within separate availability zones to safeguard against data loss. • **Backup Frequency:** Incremental backups performed daily and full backups conducted weekly. • **Retention Policy:** Backups retained for a minimum of 90 days or as directed by the State's data retention policies. • **Verification:** Regular automated and manual validation of backup integrity and recoverability. All backup processes will be fully auditable, with logs accessible to the State upon request. **Disaster Recovery and Restoration Procedures** SpruceID will maintain a comprehensive Disaster Recovery Plan (DRP) that defines recovery point objectives (RPOs) and recovery time objectives (RTOs) aligned with the State's SLA. • **Target RPO:** ≤ 24 hours (maximum acceptable data loss window). • **Target RTO:** ≤ 12 hours (maximum acceptable downtime for service restoration). Disaster recovery procedures will include clear roles, escalation protocols, and step-by-step restoration processes to ensure rapid recovery in the event of data corruption, infrastructure failure, or cybersecurity incident. DR testing will be conducted at least annually—or more frequently if requested by the State—to validate readiness and identify opportunities for improvement. **Verification, Reporting, and Continuous Improvement** The State of West Virginia will receive verification reports summarizing backup schedules, DR test results, and SLA performance metrics on a quarterly basis. Any deviation from recovery objectives will be immediately reported, and corrective

	actions will be documented and tracked to resolution. By maintaining a comprehensive, secure, and verifiable business continuity and disaster recovery strategy, SpruceID ensures that the One-Stop-Shop Permitting Portal will remain operational, resilient, and fully compliant with the State's data integrity and continuity 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.	SpruceID affirms that the proposed solution will be fully capable of being migrated into one of the State of West Virginia's existing cloud tenants upon completion of development and acceptance. The system's modular, standards-based architecture is designed to support flexible deployment options, including migration from SpruceID's implementation environment to a State-managed Microsoft Azure Government, AWS GovCloud (US), or other approved cloud tenant without loss of functionality or data integrity. **Migration Readiness and Compatibility** The One-Stop-Shop Permitting Portal will be developed within a cloud-agnostic framework that adheres to infrastructure-as-code (IaC) principles, allowing for seamless replication of configurations, services, and security controls within the State's environment. All application components—including the web application, APIs, databases, and storage layers—will be containerized or virtualized for portability across FedRAMP-authorized cloud providers. System configuration, access policies, and infrastructure templates will be fully documented to enable State IT personnel or authorized administrators to deploy the solution within their existing tenant environment. This documentation will include: • Network architecture diagrams and virtual network configurations; • Security group and identity access management (IAM) settings; • Storage, database, and encryption key management details; and • Deployment scripts and environment variable definitions. **Data Migration and Validation** SpruceID will coordinate closely with the West Virginia Office of Technology (WVOT) to ensure that all data migration activities comply with State cybersecurity and data-handling requirements. Prior to migration, a complete data export—including application metadata, audit logs, and document repositories—will be performed and validated using checksums and reconciliation reports to confirm accuracy and integrity. All data transfers will be encrypted in transit using TLS 1.2+ and verified against FIPS 140-3 cryptographic standards. Post-migration, SpruceID will assist in validation testing to confirm that the system functions identically in the State's tenant and that all integrations, workflows, and permissions remain intact. **Ongoing Support and Transition Assistance** SpruceID will provide technical assistance during and immediately after the migration process to ensure a smooth transition. Our team will remain available to support environment setup, security verification, and troubleshooting until the State

	confirms successful deployment and continuity of operations. By designing the One-Stop-Shop Permitting Portal to be cloud-portable, standards-compliant, and fully documented, SpruceID ensures that the solution can be seamlessly migrated into the State's existing cloud tenant—providing the State of West Virginia with long-term control, flexibility, and operational independence.
4.2.2.12 Vendor must make the project management interface available and accessible to the State's implementation team at no additional cost	SpruceID affirms that the project management interface and collaboration tools used for this project will be made fully available and accessible to the State's implementation team at no additional cost. The State will be granted continuous access to the project management environment throughout all phases of implementation, including discovery, development, testing, deployment, and post-launch support. This access will allow authorized State personnel to view project schedules, task assignments, progress metrics, sprint reports, issue logs, and documentation in real time. SpruceID currently utilizes Linear as its primary project management platform but can readily integrate with or transition to the State's preferred system (e.g., Jira, Trello, Asana, Smartsheet, or Microsoft Project) upon request, without any additional cost to the State. All project documentation and progress records will remain transparent and readily accessible to designated State stakeholders for the duration of the contract. By maintaining open access to the project management interface, SpruceID ensures full visibility, accountability, and collaboration with the State's implementation team—supporting effective oversight, timely communication, and shared ownership of project milestones.
4.2.2.13 Vendor's solution must provide a real-time data exchange.	SpruceID's proposed solution will provide a secure, standards-based real-time data exchange framework that enables seamless interoperability between the One-Stop-Shop Permitting Portal and participating agency systems. This capability ensures that data entered, updated, or approved in one system is immediately reflected across all connected environments, reducing manual reconciliation and improving transparency for both agencies and applicants. **Architecture and Standards** The solution will employ a RESTful API architecture with support for JSON and XML data formats, enabling reliable two-way communication between the central permitting platform and agency or third-party systems. Real-time synchronization will be achieved through event-driven APIs and webhooks, which automatically trigger updates when defined actions occur—such as application submission, status changes, or payment confirmation. All API endpoints will be secured with TLS 1.2+ encryption and authenticated via OAuth 2.0 or mutual TLS (mTLS). Access will be controlled through role-based permissions and audit logging to ensure that only authorized systems and users can initiate or receive data exchanges. In addition to RESTful APIs, the platform will support secure file transfer (SFTP), message queue–based exchange, and asynchronous batch ingestion for legacy systems. This ensures interoperability even where agencies rely on non-API systems. All integration channels are encrypted using TLS 1.2+ and use FIPS 140-3 validated cryptography, consistent with WVOT security architecture.

	Data Exchange Capabilities Real-time data exchange will support, but not be limited to, the following interactions: • Submission and retrieval of application data between agencies; • Synchronization of permit status, inspection results, and approvals; • Integration with payment processors for transaction confirmations; • Communication with document repositories, GIS systems, or other external services; and • Updates to dashboards and reporting tools for immediate visibility into program metrics. These integrations will ensure that all agencies operate on a consistent, up-to-date dataset, improving decision-making and eliminating redundant data entry. **Performance and Reliability** The system will include built-in monitoring to ensure high performance and reliability of all data exchange operations. Message queues and retry mechanisms will maintain data consistency even if a connected system experiences temporary downtime, with all transactions logged for traceability and reconciliation. By implementing a real-time, secure, and standards-compliant data exchange, SpruceID's solution will enable the State of West Virginia to achieve full interoperability across its permitting ecosystem—supporting transparency, efficiency, and data integrity across all connected agencies and systems.
4.2.2.14 Vendor's solution must be ADA compliant and meet the updated federal requirements.	SpruceID affirms that the proposed solution will be fully compliant with the Americans with Disabilities Act (ADA) and all updated federal accessibility requirements, ensuring equal access for all users, including individuals with disabilities. The One-Stop-Shop Permitting Portal will be designed, developed, and tested in alignment with the latest Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, as referenced by Section 508 of the Rehabilitation Act and applicable ADA Title II digital accessibility requirements. SpruceID will produce a full VPAT for the permitting portal before launch and maintain as a part of ongoing accessibility compliance. **Accessibility by Design** Accessibility will be integrated from the earliest stages of design through final deployment. The user interface, navigation, and content will be developed using inclusive design principles that accommodate a wide range of abilities and assistive technologies. All interactive elements—including forms, buttons, menus, and dashboards—will be optimized for keyboard navigation, screen readers, and high-contrast display modes. **Testing and Validation** SpruceID will conduct automated and manual accessibility testing throughout the

	development process. Testing will include the use of assistive technologies such as JAWS, NVDA, and VoiceOver to verify compliance with accessibility requirements. Prior to launch, a full accessibility review will be completed, and the State will receive documentation confirming adherence to ADA and WCAG standards. Accessibility testing will continue post-launch as part of SpruceID's quality assurance process, with regular updates to address evolving standards and user feedback. Any identified accessibility issues will be prioritized for resolution consistent with the State's service-level expectations. **Ongoing Compliance and Reporting** SpruceID will maintain accessibility as a standing requirement for all system enhancements and new feature releases. Updates to ADA or WCAG standards will be monitored, and the platform will be adjusted proactively to maintain continuous compliance. The State may request accessibility conformance reports (ACRs) or Voluntary Product Accessibility Templates (VPATs) at any time. By embedding accessibility into every stage of design, testing, and maintenance, SpruceID ensures that the One-Stop-Shop Permitting Portal will be fully ADA compliant, user-friendly, and accessible to all West Virginians, in accordance with the most current federal digital accessibility requirements.
4.2.2.15 Vendor must provide 3-tier outage reporting.	SpruceID's proposed solution will include a structured, three-tier outage reporting process that ensures timely, transparent communication with the State of West Virginia regarding any service interruptions or performance degradation. This framework provides clear escalation paths, defined response timelines, and detailed reporting for all incident severities in accordance with the Service Level Agreement (SLA). **Tier 1 — Critical Outage (Severe Impact)** A Tier 1 outage is defined as a complete system failure or loss of access affecting all users and critical business functions. • **Response Time:** Immediate notification to the State within 30 minutes of detection. • **Resolution Target:** Service restoration within 4 hours, with continuous updates provided every hour until resolved. • **Post-Incident Reporting:** A detailed root-cause analysis (RCA) and corrective action report delivered within 3 business days of restoration. **Tier 2 — Major Degradation (Partial Impact)** A Tier 2 outage represents partial functionality loss, reduced performance, or disruption affecting one or more key subsystems (e.g., payment processing, form submission, or dashboard availability). • **Response Time:** Notification to the State within 1 hour of detection. • **Resolution Target:** Service restoration within 8 hours, with updates every 2 hours until resolved. • **Post-Incident Reporting:** Summary of issue, resolution steps, and

	follow-up actions provided within 5 business days. **Tier 3 — Minor Disruption (Limited Impact)** A Tier 3 outage involves isolated, low-impact incidents such as delayed notifications, minor interface issues, or brief connectivity interruptions that do not materially affect system operations. • **Response Time:** Notification to the State within 4 business hours of detection. • **Resolution Target:** Correction within 2 business days, or inclusion in the next scheduled maintenance release. • **Post-Incident Reporting:** Included in the next scheduled maintenance or performance summary report. **Transparency and Reporting** All outages and performance incidents will be logged, categorized, and tracked in SpruceID's incident management system. The State will have direct access to real-time status dashboards and outage notifications via email and/or SMS. Comprehensive quarterly uptime and incident summary reports will be provided to the West Virginia Office of Technology (WVOT) for performance review and compliance verification. By implementing this three-tier outage reporting model, SpruceID ensures rapid response, transparent communication, and continuous accountability—maintaining high system availability and trust in the One-Stop-Shop Permitting Portal's reliability.
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.	SpruceID will provide the State's implementation team with early and continuous access to both sandbox and production environments to support collaboration, testing, and validation throughout the development lifecycle. This approach promotes transparency, accelerates feedback, and ensures that the One-Stop-Shop Permitting Portal meets the State's operational requirements from the outset. **Sandbox Environment** A fully functional sandbox (testing) environment will be provisioned early in Phase 2 of the project (Design and Prototyping) to allow the State's technical and program staff to: • Review evolving features and configurations in real time; • Conduct user acceptance testing (UAT) and workflow validation; • Test integrations with existing agency systems and APIs; and • Provide feedback to guide iterative development. The sandbox environment will mirror the production configuration—including authentication, data models, and workflows—while remaining logically isolated to protect live data. All test data will be encrypted and managed in accordance with

	State security requirements. **Production Environment** As development advances, SpruceID will also provide controlled access to the production environment for designated State personnel prior to formal launch. This will enable the State to perform operational readiness checks, configuration reviews, and data validation prior to go-live. Both environments will be hosted within FedRAMP-authorized cloud infrastructure and maintained under strict access control policies. The State will have administrative or read-only permissions appropriate to each phase, with all actions logged for audit and compliance purposes.
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.	SpruceID will provide the State of West Virginia with a comprehensive Disentanglement Plan within six (6) months of contract award, in full compliance with the requirements outlined in Attachment A of this solicitation. The plan will ensure a smooth and orderly transition of services, data, and system assets to the State or a successor vendor at the conclusion of the contract term or upon request. The plan will include: • Full export of all data in State-specified formats; • Transfer of all workflows, configurations, and form schemas; • Delivery of IaC templates, deployment scripts, and cloud configuration; • Turnover of all logs, audit trails, and security artifacts; • Knowledge-transfer sessions for the State or successor vendor; • Assistance with environment teardown or handoff as directed by WVOT. All disentanglement activities will occur without interruption to State operations.
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.	SpruceID's proposed solution will include comprehensive, ongoing support and maintenance services for the full duration of the contract. These services ensure that the One-Stop-Shop Permitting Portal remains secure, reliable, and continuously aligned with the State of West Virginia's operational, security, and performance objectives. **Scope of Support and Maintenance** SpruceID will provide proactive and responsive technical support covering all aspects of system performance, functionality, and security. This includes: • **Routine Updates and Enhancements:** Regular software updates, performance tuning, and feature improvements to maintain compliance with State and federal standards. • **Bug Fixes and Corrective Maintenance:** Timely resolution of defects and identified issues consistent with agreed service-level timelines. • **Security Patching:** Ongoing vulnerability monitoring and patch deployment to maintain continuous system protection.

- **Compatibility Assurance:** Regular validation of compatibility with modern browsers, devices, accessibility standards, and integrated systems.

Dedicated Technical Customer Success Manager

SpruceID will assign a Technical Program Manager (TPM) to serve as the State's primary technical point of contact throughout the contract. The TPM will:

- Oversee day-to-day coordination of support and maintenance activities;
- Facilitate communication between SpruceID's engineering, product, and support teams and the State's technical staff;
- Track open issues, feature requests, and performance metrics;
- Conduct quarterly success reviews and ensure continuous alignment with the State's program goals; and
- Coordinate proactive recommendations for system optimization and upcoming releases.

This dedicated role ensures that the State receives personalized, proactive support and a consistent liaison for all technical matters, reinforcing accountability and responsiveness.

Support Availability and Service Levels

SpruceID will provide a dedicated support channel accessible to authorized State personnel via email, phone, or ticketing portal. Support will be available during standard business hours, with 24/7 on-call escalation for critical incidents. Response and resolution times will adhere to the agreed-upon service-level commitments defined in the contract.

Continuous Improvement and Lifecycle Management

SpruceID will collaborate with the State's implementation and IT teams to regularly evaluate system usage, performance, and user feedback. These insights will guide iterative improvements, ensuring the platform continues to meet evolving State needs. All maintenance activities—including updates and patches—will be scheduled transparently and conducted outside of business hours to minimize disruption, consistent with Section 4.2.1.20.

By providing comprehensive maintenance services, dedicated technical account oversight through a Technical Customer Success Manager, and a commitment to proactive improvement, SpruceID ensures the One-Stop-Shop Permitting Portal remains a secure, high-performing, and continuously optimized system throughout the contract term.

VI. Qualifications and Experience

Desired Requirement	Our Response
4.3.1.1. Vendors should highlight a Proven track record designing, deploying, or supporting permitting platforms for state or local agencies.	SpruceID brings a proven track record of designing, deploying, and supporting permitting and credentialing platforms for government agencies at the state and local levels. Our work with the State of Utah's Verifiable Digital Credentials (VDC) Initiative serves as a primary example of our ability to deliver secure, standards-based permitting solutions that enhance efficiency, interoperability, and citizen experience across diverse use cases. **Utah Statewide VDC Initiative** SpruceID served as the primary technical partner to the State of Utah in implementing the Utah Verifiable Digital Credentials (VDC) program, a statewide initiative established under legislative direction in Utah Code §63A-16-110 et seq. The law required the Department of Government Operations to create a privacy-preserving, interoperable system for issuing and verifying digital credentials across all state agencies. SpruceID architected and deployed the VDC platform in direct response to this legislative mandate, enabling multiple agencies to issue and manage secure, verifiable digital credentials in a standardized manner. The initiative was designed to serve as the foundation for statewide modernization—allowing agencies to digitize existing permits, licenses, and certifications through a shared infrastructure that ensures compliance, scalability, and resident trust. **Representative Use Cases** The Utah VDC system supports a variety of real-world permitting and certification workflows that closely align with the State of West Virginia's goals for the One-Stop-Shop Permitting Portal. Examples include: • **Off-Highway Vehicle (OHV) Education Permits:** Digital issuance and verification of safety education certificates for recreational vehicle operators. The system enables instant, offline-capable, credential validation by enforcement officers, eliminating the need for paper certificates and reducing administrative overhead. • **Food Handler Permits:** Digitally issued and verifiable credentials for certified food handlers, allowing individuals to share credentials with employers or inspectors through QR code or barcode verification. This streamlined process simplifies renewals, enhances compliance, and supports interoperability with local health departments. • **Liquefied Petroleum Gas (LPG) Certificates:** Secure, digital certification for licensed professionals managing propane and other gas systems. Credentials can be instantly verified in the field via mobile devices, improving safety oversight and ensuring regulatory compliance. Each of these use cases demonstrates SpruceID's ability to integrate complex, multi-agency workflows within a unified, user-friendly digital framework. The VDC platform's modular architecture allows for seamless onboarding of new permit types, enabling rapid scaling across agencies and programs. **Results and Impact** The Utah VDC program has been recognized nationally as a model for statewide interoperability, privacy-preserving design, and digital modernization. By digitizing permits and licenses across multiple regulatory domains, the State has reduced

Desired Requirement	Our Response
4.3.1.1. Vendors should highlight a Proven track record designing, deploying, or supporting permitting platforms for state or local agencies.	SpruceID brings a proven track record of designing, deploying, and supporting permitting and credentialing platforms for government agencies at the state and local levels. Our work with the State of Utah's Verifiable Digital Credentials (VDC) Initiative serves as a primary example of our ability to deliver secure, standards-based permitting solutions that enhance efficiency, interoperability, and citizen experience across diverse use cases. **Utah Statewide VDC Initiative** SpruceID served as the primary technical partner to the State of Utah in implementing the Utah Verifiable Digital Credentials (VDC) program, a statewide initiative established under legislative direction in Utah Code §63A-16-110 et seq. The law required the Department of Government Operations to create a privacy-preserving, interoperable system for issuing and verifying digital credentials across all state agencies. SpruceID architected and deployed the VDC platform in direct response to this legislative mandate, enabling multiple agencies to issue and manage secure, verifiable digital credentials in a standardized manner. The initiative was designed to serve as the foundation for statewide modernization—allowing agencies to digitize existing permits, licenses, and certifications through a shared infrastructure that ensures compliance, scalability, and resident trust. **Representative Use Cases** The Utah VDC system supports a variety of real-world permitting and certification workflows that closely align with the State of West Virginia's goals for the One-Stop-Shop Permitting Portal. Examples include: • **Off-Highway Vehicle (OHV) Education Permits:** Digital issuance and verification of safety education certificates for recreational vehicle operators. The system enables instant, offline-capable, credential validation by enforcement officers, eliminating the need for paper certificates and reducing administrative overhead. • **Food Handler Permits:** Digitally issued and verifiable credentials for certified food handlers, allowing individuals to share credentials with employers or inspectors through QR code or barcode verification. This streamlined process simplifies renewals, enhances compliance, and supports interoperability with local health departments. • **Liquefied Petroleum Gas (LPG) Certificates:** Secure, digital certification for licensed professionals managing propane and other gas systems. Credentials can be instantly verified in the field via mobile devices, improving safety oversight and ensuring regulatory compliance. Each of these use cases demonstrates SpruceID's ability to integrate complex, multi-agency workflows within a unified, user-friendly digital framework. The VDC platform's modular architecture allows for seamless onboarding of new permit types, enabling rapid scaling across agencies and programs. **Results and Impact** The Utah VDC program has been recognized nationally as a model for statewide interoperability, privacy-preserving design, and digital modernization. By digitizing permits and licenses across multiple regulatory domains, the State has reduced

	administrative processing time, improved verification accuracy, and provided residents with a more convenient, secure way to access essential government services. SpruceID's experience in Utah directly informs our proposed approach for the State of West Virginia. The same standards-based, modular architecture and user-centered design principles will guide the development of West Virginia's One-Stop-Shop Permitting Portal, ensuring a modern, scalable solution built on demonstrated success. SpruceID's experience delivering this system under a legislative deadline directly parallels the State of West Virginia's statutory requirement under W. Va. Code §5A-13-1 et seq., which calls for full implementation of a unified permitting platform by January 1, 2027. Our team's firsthand experience operating within a similar policy framework ensures that our proposed solution will not only meet technical specifications but also align with the State's legal, operational, and governance obligations.
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.	SpruceID has extensive experience integrating modern digital platforms with legacy systems, middleware, and third-party applications in state and local government environments. Our approach emphasizes secure, standards-based data exchange using APIs and event-driven architectures to ensure interoperability without disrupting mission-critical operations. **California Department of Motor Vehicles (DMV) – Legacy Integration** SpruceID served as the primary implementer for the California Department of Motor Vehicles (DMV) mobile driver's license (mDL) and identity modernization initiative, where the team successfully integrated new digital credentialing components into the DMV's complex legacy infrastructure. The project required interoperability with multiple backend systems—spanning modern cloud services and decades-old mainframe applications—while maintaining compliance with strict State of California security and privacy mandates. To achieve this, SpruceID worked with the agency's integration team utilizing MuleSoft, the State's enterprise middleware platform, to broker communication between the new mDL application and the DMV's Salesforce-based customer relationship management (CRM) system and legacy mainframe system of record. This architecture allowed real-time data exchange for credential issuance, verification, and audit tracking, without requiring major modification of the existing systems. Our integration framework supported: • **RESTful and SOAP API communication** between modern and legacy endpoints; • **Secure token-based authentication** (OAuth 2.0 and mTLS) for inter-system communication; • **Message transformation and routing** through MuleSoft to standardize data models; • **Data synchronization** between Salesforce CRM and the new mDL issuance platform; and • **Error handling and monitoring** to ensure reliability and full auditability

	across the entire data flow. This work demonstrated SpruceID's ability to deliver modernization in a high-stakes, data-sensitive environment—enabling California to extend new digital credentialing capabilities while maintaining the continuity of its core legacy systems. **Approach and Technical Capabilities** Across all state engagements, SpruceID follows a modular integration strategy that prioritizes security, performance, and future scalability. Our solutions support both real-time and batch data exchanges through: • **RESTful and GraphQL APIs** for modern systems; • **Middleware connectors** (e.g., MuleSoft and similar) for legacy and hybrid environments; • **Secure file transfer and message queuing** for systems that do not expose APIs; and • **Standards-based data schemas** (JSON, XML) to ensure interoperability across platforms. All integrations are encrypted in transit using TLS 1.2+ and leverage FIPS 140-3 validated cryptographic modules for compliance with federal and State cybersecurity policies. **Relevance to West Virginia** SpruceID's experience integrating with both modern middleware and legacy mainframes positions the team to seamlessly connect the proposed One-Stop-Shop Permitting Portal with West Virginia's existing permitting, payment, and agency record systems. Our approach will allow the State to achieve real-time interoperability across systems of record while preserving existing investments and minimizing operational disruption. By combining modern API-driven design with deep familiarity in state-level legacy system integration, SpruceID ensures that West Virginia's permitting modernization effort will be both technically feasible and operationally sustainable from day one.
4.3.1.3. Vendors should describe Familiarity with scalable, secure cloud platforms (e.g., Azure, AWS, Google Cloud) and disaster recovery best practices.	SpruceID has extensive experience architecting, deploying, and managing scalable, secure solutions across major commercial cloud platforms—including Amazon Web Services (AWS) and Microsoft Azure. These platforms form the foundation for SpruceID's current production environments and client deployments, supporting millions of digital transactions with high availability and robust data protection. **Cloud Infrastructure Expertise** SpruceID's engineering team has deep expertise in designing cloud architectures that balance security, performance, and cost efficiency. Our experience spans: • **AWS:** Use of core services such as EC2, ECS, EKS, RDS, S3, CloudFront, and KMS for secure storage, compute scalability, and encryption key management.

- **Microsoft Azure:** Deployment of containerized applications using Azure App Services, Azure Active Directory integration for SSO and RBAC, and use of Azure Monitor and Sentinel for security oversight.

All environments will be configured in alignment with NIST SP 800-53 Rev. 5 control baselines and FIPS 140-3 validated encryption modules, ensuring compliance with State and federal security expectations.

Scalability and Performance

SpruceID's proposed architecture leverages containerized services to achieve elastic scalability across all supported cloud platforms. Using cloud-native technologies such as orchestrators (e.g. Kubernetes, ECS), content delivery networks (CDNs), and managed storage solutions (e.g. RDS, S3), the proposed system dynamically adjusts compute and storage resources in response to demand—ensuring consistent performance even during peak permitting periods or system updates.

High availability is achieved through multi-datacenter deployments with automatic failover.

Disaster Recovery and Business Continuity

SpruceID follows industry-standard disaster recovery (DR) best practices to ensure business continuity and data integrity across all deployments. Our DR approach includes:

- Automated daily and incremental backups, encrypted and stored in separate regions for redundancy;
- Recovery Point Objective (RPO) of ≤ 24 hours and Recovery Time Objective (RTO) of ≤ 12 hours;
- Regular failover testing and validation of backup restoration procedures; and
- Comprehensive monitoring and alerting using native cloud tools (e.g., AWS CloudWatch, Azure Monitor).

This approach ensures that all application and data layers can be restored rapidly and verifiably in the event of an outage or disruption.

By leveraging proven, commercially available cloud platforms—AWS, Azures—SpruceID's proposed solution provides the State of West Virginia with a secure, scalable, and cost-efficient infrastructure that aligns with existing State IT operations. The system's architecture supports seamless migration into the State's preferred cloud tenant (as detailed in Section 4.2.2.11) while meeting all State cybersecurity and continuity requirements.

SpruceID's cross-platform experience ensures that the One-Stop-Shop Permitting Portal will operate on a flexible, resilient, and standards-compliant cloud foundation, capable of scaling to meet future growth and service demands.

4.3.1.4. Vendors should explain their experience managing sensitive data with encryption, access controls, and audit trails.	SpruceID has extensive experience designing and operating systems that manage sensitive personal and regulatory data for state and federal programs, with strict adherence to privacy, security, and compliance standards. Across all deployments, SpruceID implements a layered, defense-in-depth model encompassing encryption, role-based access controls (RBAC), and comprehensive audit logging—ensuring that sensitive information remains protected, traceable, and recoverable throughout its lifecycle. **Data Encryption** All sensitive data handled within SpruceID's platforms is encrypted both at rest and in transit using FIPS 140-3 validated algorithms. Data stored in databases, backups, and file systems is encrypted using AES-256, while all network traffic between users, applications, and integrated systems is protected using Transport Layer Security (TLS) 1.2 or higher. Encryption keys are managed through secure key management services (KMS) within cloud environments, with automated key rotation, separation of duties, and strict access logging. This configuration aligns with NIST SP 800-53 Rev. 5 controls and State cybersecurity standards. **Access Controls** SpruceID employs a least-privilege access model across all environments. Users—whether State personnel, agency administrators, or SpruceID support staff—will be granted only the permissions required for their role. Multi-factor authentication (MFA) will be enforced for all administrative access, and access to production data will be tightly restricted to authorized, U.S.-based personnel. Role-Based Access Control (RBAC) will be configurable at both the system and application levels, enabling fine-grained management of permissions. Each agency can define its own access policies, ensuring that internal segregation of duties and audit requirements are met. **Audit Logging and Traceability** SpruceID's proposed systems maintain comprehensive audit trails for all access, configuration, and data modification events. Logs are immutable, time-stamped, and securely stored in accordance with NIST, FedRAMP, and ISO/IEC 27001 best practices. The audit framework provides: • Full visibility into user authentication events, system configuration changes, and data access requests; • Tamper-evident logging mechanisms with cryptographic integrity checks; and • Reporting tools that allow authorized administrators and auditors to review activity by user, time, and event type. Audit data will be retained in accordance with the State's record retention policies and can be exported into the State's existing Security Information and Event Management (SIEM) system for centralized monitoring and incident response. **Demonstrated Performance in Sensitive Environments**

	SpruceID's proven success managing sensitive data for state-level programs—such as the Utah Verifiable Digital Credentials (VDC) Initiative and the California DMV mobile driver's license (mDL) modernization—illustrates our ability to maintain strict data protection and auditability requirements under regulatory oversight. By applying this same security discipline to the One-Stop-Shop Permitting Portal, SpruceID will ensure that all constituent, agency, and operational data remains confidential, integrity-protected, and fully auditable, in full compliance with the State of West Virginia's cybersecurity and privacy expectations.
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.	SpruceID has experience partnering with state agencies to secure and maintain its software in alignment with all necessary compliance requirements. As part of its overall solutions training, we include training on key control families, including Access Control, System and Communications Protection, Incident Response (IR), and more. These training programs ensure teams understand what users need to know for how to apply the controls in daily operations, maintain secure configurations, manage vulnerabilities effectively, and respond quickly to emerging threats.
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.	SpruceID has extensive experience managing large-scale government technology projects using a tailored, collaborative project management approach that adapts to the specific needs, culture, and workflows of each agency partner. Our methodology combines agile delivery principles with structured reporting and documentation practices—ensuring transparency, accountability, and consistent progress toward milestones. **Adaptable Project Management Framework** SpruceID's standard project management framework is built around Agile and hybrid methodologies, allowing iterative development and early validation while maintaining the formal controls often required in public-sector environments. This flexibility enables us to align with each agency's internal review cadence, procurement policies, and reporting requirements. Our approach emphasizes: • Clear definition of roles, responsibilities, and communication channels; • Incremental delivery through short development sprints; • Regular progress reviews and milestone tracking; • Joint risk management and issue resolution; and • Continuous stakeholder engagement throughout all phases of implementation. **Tool Compatibility and Transparency** SpruceID currently utilizes Linear as its internal project management and sprint-tracking tool but is fully capable of and committed to adopting the State's preferred tools at no additional cost. Our team has experience managing projects in environments that use:

	• **Jira** – for agile sprint management, issue tracking, and backlog prioritization; • **Smartsheet** – for milestone tracking, cross-agency coordination, and reporting dashboards; • **Microsoft Project** – for Gantt-based scheduling, resource allocation, and critical-path analysis; and • **Trello or Asana** – for task management and visual collaboration. All project data—tasks, timelines, deliverables, and documentation—will remain accessible to the State's implementation team in real time, ensuring complete visibility and collaborative oversight. **Customization and Agency Collaboration** SpruceID will collaborate with the State's project management office (PMO) and participating agencies to establish a governance framework that reflects the State's operational structure. This may include joint project boards, shared dashboards, and customized reporting templates. The project plan and associated tools will be configured to match each agency's workflow, approval process, and communication preference. By offering a flexible, tool-agnostic, and transparent project management approach, SpruceID ensures that the State of West Virginia's implementation team can monitor progress, manage dependencies, and coordinate multi-agency input efficiently throughout the One-Stop-Shop Permitting Portal project.
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.	SpruceID has a demonstrated history of developing and executing successful train-the-trainer programs and on-demand training portals for both agency staff and public users. Our approach focuses on building sustainable internal capacity—empowering State teams to manage, operate, and expand digital systems long after initial implementation—while ensuring that residents can easily navigate and adopt new digital services. **Utah Verifiable Digital Credentials (VDC) Initiative – Train-the-Trainer Success** As part of the Utah Verifiable Digital Credentials (VDC) statewide initiative, SpruceID partnered closely with the Utah Department of Government Operations (GovOps) to design and implement a comprehensive training and knowledge-transfer program for agency stakeholders. Following deployment of the initial credentialing workflows, SpruceID collaborated with GovOps to: • Develop detailed implementation guides, step-by-step workflow manuals, and reference materials tailored to each participating agency; • Conduct hands-on training sessions and train-the-trainer workshops that equipped agency leads with the knowledge and confidence to onboard their own staff; • Establish an on-demand digital resource portal where agency personnel could access materials and review updates at their convenience.

	This model proved essential as additional agencies—ranging from the Department of Natural Resources to the Department of Health—began implementing their own digital permit and certification workflows under the VDC framework. By creating reusable documentation and scalable learning content, SpruceID and GovOps reduced dependence on vendor-led training and accelerated adoption across multiple departments. **Approach and Sustainability** SpruceID applies the same proven methodology to all engagements, combining: • Structured train-the-trainer programs that produce knowledgeable internal champions within each agency; • Modular learning materials that can be updated as workflows evolve; and • Accessible, self-paced training portals for ongoing education and refreshers for both internal users and the public. All materials are compliant with WCAG 2.1 AA accessibility standards, ensuring that resources are usable by individuals of all abilities. This experience directly informs our approach for the West Virginia One-Stop-Shop Permitting Program. SpruceID will deliver a similar, scalable training framework—equipping agency leads to train their teams independently and maintaining an on-demand learning portal to support continued education for both agency personnel and constituents. By leveraging our proven partnership model from Utah GovOps, SpruceID will ensure that the State of West Virginia has a self-sustaining, accessible, and scalable training ecosystem that supports successful system adoption and long-term operational independence.
4.3.1.8. Vendors should demonstrate familiarity with uptime guarantees, RTO/RPO metrics, and service-level reporting.	Our familiarity with these metrics is demonstrated through prior state implementations and is reflected in the business continuity, disaster recovery, and availability frameworks described in Sections 4.2.1.20 and 4.2.2.10 of this proposal. **Uptime and Service-Level Commitments** SpruceID's systems are architected to maintain 99.9% or greater uptime, excluding scheduled maintenance windows, ensuring continuous access for both agency users and the public. High availability is achieved through multi-region redundancy, load balancing, and continuous monitoring of system health. These mechanisms were outlined in our earlier responses and will apply equally to the West Virginia One-Stop-Shop Permitting Portal. In prior deployments, SpruceID successfully met or exceeded uptime commitments for both production and sandbox environments, with transparent reporting and real-time service dashboards provided to agency stakeholders. **Recovery Time and Recovery Point Objectives (RTO/RPO)** As detailed in Section 4.2.2.10, SpruceID's disaster recovery plan defines measurable recovery objectives:

	• Recovery Point Objective (RPO): ≤ 24 hours — ensuring minimal data loss in the event of a system interruption; • Recovery Time Objective (RTO): ≤ 12 hours — guaranteeing restoration of critical services within half a business day. These metrics are tested regularly through controlled failover simulations and verified against automated monitoring systems to ensure accuracy and readiness. **Service-Level Reporting and Transparency** SpruceID maintains a structured service-level reporting framework that provides the State with regular visibility into system performance. Monthly and quarterly SLA reports will include: • Uptime and availability statistics; • Incident and outage summaries with resolution timelines; • Security patch and maintenance logs; and • Verification of compliance with agreed RTO/RPO targets. The State will also have access to live dashboards and outage notifications to monitor uptime in real time. Post-incident reports, including root cause analyses (RCAs), will be delivered following any critical event to ensure accountability and continuous improvement.
4.3.1.9. Vendors should explain experience working with multi-agency teams, gathering requirements, and managing change.	SpruceID has extensive experience working with multi-agency teams in state government environments, leading complex modernization projects that require coordination across diverse stakeholders, legacy systems, and policy domains. Our work with both the Utah Department of Government Operations (GovOps) on the Verifiable Digital Credentials (VDC) statewide initiative and the California Department of Motor Vehicles (DMV) on the mobile driver's license (mDL) and digital identity modernization project demonstrates our ability to align technical execution with policy, operational, and organizational priorities across agencies. **Utah Verifiable Digital Credentials (VDC) Initiative** Under a legislative mandate (Utah Code §63A-16-110 et seq.), SpruceID partnered with Utah GovOps to develop a statewide platform enabling multiple agencies—including the Department of Commerce, Department of Natural Resources, and Department of Health—to issue and verify digital permits and licenses. SpruceID led multi-agency coordination sessions to define cross-department workflows, interoperability requirements, and data governance frameworks. We worked closely with each participating agency to document business rules, approval chains, and system dependencies, ensuring the final solution could adapt to each agency's statutory and operational context. Key components of this collaboration included: • Facilitating requirements workshops and stakeholder interviews to capture distinct agency processes and compliance obligations; • Developing shared data models to enable secure inter-agency data exchange;

- Managing change control processes as agencies transitioned from paper-based and siloed systems to digital credential issuance; and
- Conducting joint testing and validation with agency users before each rollout.

This structured approach allowed multiple agencies to join the platform in phases while maintaining consistent security, privacy, and user experience standards.

California DMV Digital Modernization

SpruceID also played a central technical and stakeholder coordination role in the California DMV's mDL initiative, which modernized the State's driver licensing and identity verification ecosystem. The project involved deep collaboration across multiple entities— including the California Department of Technology, Office of Digital Innovation, Department of Homeland Security (DHS), and Transportation Security Administration (TSA)—as well as the DMV's own internal technology and policy teams.

SpruceID worked closely with the DMV's Mulesoft integration platform, Salesforce CRM, and mainframe system of record to design secure, real-time data exchange between legacy systems and the new mobile credentialing infrastructure. Beyond the technical integration, SpruceID led public education and inter-agency readiness sessions to ensure statewide understanding and acceptance of the new credential format.

These outreach efforts included:

- Hosting education and awareness sessions for the general public and for partner agencies responsible for accepting or verifying mobile driver's licenses (mDLs), such as law enforcement, airport authorities, and licensing boards;
- Developing plain-language guides and demonstration materials to clarify how digital credentials would be presented and verified; and
- Facilitating inter-agency pilots to validate real-world interoperability and user experience.

SpruceID also partnered with the Transportation Security Administration (TSA) during mDL testing at the Transportation Security Integration Facility (TSIF) to ensure that California-issued mDLs could be verified at TSA security checkpoints in accordance with ISO/IEC 18013-5 standards. This collaboration included end-to-end testing of the credential presentation and verification flows between the DMV system and TSA's secure verification environment—making California one of the first states to successfully validate mDL acceptance in live operational conditions.

These combined activities demonstrate SpruceID's ability to manage multi-stakeholder programs that require not only technical integration but also broad public communication, regulatory coordination, and adoption management across agencies.

Change Management and Stakeholder Engagement Approach

Across all engagements, SpruceID employs a structured change-management framework that includes early stakeholder involvement, transparent communication, and continuous training. Our approach ensures that every agency—not just early

	adopters—feels ownership of the process and confidence in the resulting system. By leveraging lessons learned from Utah's multi-agency credentialing rollout and California's enterprise-scale system integration, SpruceID brings a proven methodology for cross-agency coordination, requirements definition, and managed change, ensuring the West Virginia One-Stop-Shop Permitting Program is implemented efficiently, collaboratively, and with lasting institutional adoption.

Mandatory Requirement	**Our Response**
4.3.2.1. Vendor's employees must have security training and Vendor must provide records of such training upon request.	SpruceID maintains a rigorous information security and compliance program to ensure that all personnel with access to State data or project systems adhere to the highest standards of security awareness and professional conduct. **Mandatory Security Training** Every SpruceID employee and contractor is required to complete formal security awareness and data protection training prior to being granted access to any production or development environment. This training covers: • Secure data handling and privacy requirements; • Phishing awareness and social engineering prevention; • Incident reporting and escalation procedures; • Role-based access control (RBAC) principles and least-privilege enforcement; and • Compliance obligations under NIST, FedRAMP, and SOC 2 standards. Annual refresher courses are mandatory for all personnel, and completion is tracked through an internal learning management system (LMS). Additional role-specific modules are assigned for engineers, administrators, and customer success staff who manage sensitive environments or credentials. **Compliance and Documentation** SpruceID's corporate security program is audited annually under SOC 2 Type II certification, validating our adherence to the Trust Services Criteria for Security, Availability, and Confidentiality. This certification confirms that SpruceID maintains effective controls for employee training, access management, monitoring, and incident response. Comprehensive records of all employee security training—including completion certificates, curriculum content, and audit logs—are maintained and can be provided to the State of West Virginia upon request. These records demonstrate ongoing compliance with the State's cybersecurity expectations and ensure that only qualified, properly trained personnel are authorized to perform work on this project.

4.3.2.2. Vendor must highlight training in WCAG 21. and Section 508 compliance for public-facing digital services.	SpruceID is fully committed to ensuring that all public-facing digital services meet or exceed the accessibility requirements defined under the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA and Section 508 of the Rehabilitation Act. Accessibility compliance is a standardized component of every implementation we deliver. Our product and engineering teams are trained internally on accessibility best practices and integrate accessibility testing throughout the design and development process. **Accessibility Testing and Verification** Each public-facing deployment undergoes structured accessibility testing that includes: • Automated scans using industry tools (such as Axe and Lighthouse) to detect and remediate accessibility issues; • Manual review of navigation, color contrast, keyboard accessibility, and screen reader compatibility; and • User interface validation against WCAG 2.1 AA criteria for all critical user flows. Following these evaluations, SpruceID completes a Voluntary Product Accessibility Template (VPAT) to document compliance and provide transparency to our public-sector partners. VPATs are produced for every implementation and can be provided to the State upon request. **Commitment to Continuous Compliance** SpruceID monitors updates to WCAG and Section 508 standards and adjusts development practices accordingly. All accessibility findings are tracked in our issue management system, prioritized during release cycles, and verified before each new public release. By embedding accessibility testing and VPAT documentation into our standard delivery process, SpruceID ensures that the One-Stop-Shop Permitting Portal will be fully accessible, inclusive, and compliant with all federal and State digital accessibility requirements.
4.3.2.3. Vendor must show Experience aligning solutions with state IT policies, privacy laws, and accessibility mandates.	SpruceID has successfully designed and implemented digital credentialing and permitting solutions that align with state IT standards, privacy frameworks, and accessibility mandates. Our recent work with the Utah Department of Government Operations (GovOps) on the statewide Verifiable Digital Credentials (VDC) initiative and with the California Department of Motor Vehicles (DMV) on its mobile driver's license (mDL) modernization program demonstrates our ability to deliver compliant, interoperable systems within complex state policy environments. **Alignment with State IT and Security Policies** SpruceID's implementations are designed to comply with each state's enterprise IT and cybersecurity frameworks, including requirements for encryption, access control, data protection, and interoperability. In Utah, the VDC platform was deployed in alignment with the Department of Technology Services (DTS) security and interoperability standards, meeting statewide expectations for data classification, network security, and authentication.

	In California, SpruceID's integrations with the DMV's existing systems—including MuleSoft, Salesforce, and the agency's mainframe system of record—were completed in accordance with the California Department of Technology's (CDT) Statewide Information Management Manual (SIMM) and change-control procedures. These projects demonstrate SpruceID's capability to work within formal IT governance structures while introducing new, secure digital workflows. Our solutions follow established national frameworks such as NIST SP 800-53 Rev. 5, FIPS 140-3, and FedRAMP Moderate control baselines, ensuring that all implementations maintain a consistent cybersecurity posture and can interoperate with state-managed infrastructure. **Privacy and Data Protection** SpruceID applies a privacy-by-design approach across all projects, embedding privacy and data minimization principles into system architecture and workflow design. Our practices align with state-level privacy regulations, including the Utah Consumer Privacy Act (UCPA) and the California Consumer Privacy Act (CCPA), as well as federal guidance from the National Institute of Standards and Technology (NIST). Personal data is encrypted at rest and in transit, retained only as required, and always handled under strict role-based access controls. SpruceID's operations are validated through SOC 2 Type II certification, confirming adherence to the Trust Services Criteria for Security, Availability, and Confidentiality. **Accessibility and Public Inclusion** SpruceID ensures that all public-facing systems meet WCAG 2.1 Level AA and Section 508 accessibility requirements. Accessibility testing and Voluntary Product Accessibility Templates (VPATs) are part of every project delivery, ensuring that interfaces are inclusive and usable by individuals of all abilities. **Proven Policy Alignment** Through these engagements, SpruceID has demonstrated the ability to work effectively within state IT policy frameworks, manage compliance with privacy and accessibility mandates, and deliver systems that meet technical and governance standards. This experience directly informs our approach to the State of West Virginia's One-Stop-Shop Permitting Program, ensuring that the solution will be compliant, secure, and accessible from launch through long-term operation.
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).	SpruceID has demonstrated capability in implementing and maintaining strong security and operational controls across state and enterprise deployments. Our security program incorporates continuous vulnerability monitoring, encryption at all data layers, structured role-based access control (RBAC), and tested disaster recovery procedures—ensuring that systems remain resilient, auditable, and compliant with State cybersecurity expectations. **Vulnerability Scanning and Reporting** SpruceID conducts routine vulnerability scanning and security testing as part of our continuous monitoring framework. Automated scans and manual reviews are performed on infrastructure, APIs, and application code to identify and remediate vulnerabilities before release. • Vulnerability assessments are conducted at least quarterly and following

any major system update or configuration change.

- Findings are prioritized by severity using CVSS scoring and tracked to resolution in our issue management system.
- The State will receive routine vulnerability and remediation reports, and detailed summaries will be available upon request, consistent with the practices outlined in Section 4.2.2.8.

Disaster Recovery Planning and Drills

SpruceID maintains a comprehensive Business Continuity and Disaster Recovery (BC/DR) Plan, detailed in Section 4.2.2.10. This plan defines specific recovery metrics—Recovery Point Objective (RPO ≤ 24 hours) and Recovery Time Objective (RTO ≤ 12 hours)—and includes documented restoration procedures for infrastructure and data.

- Backups are encrypted, replicated across multiple regions, and validated through automated integrity checks.
- Annual DR drills are conducted to test failover procedures and confirm that all recovery objectives are achievable.
- Results of DR exercises are reviewed internally and can be shared with the State to confirm compliance.

Encryption Standards

All data managed within SpruceID's systems is encrypted in transit and at rest using Advanced Encryption Standard (AES-256) and other FIPS 140-3 validated cryptographic modules.

- Data in motion is protected using TLS 1.2 or higher, and all keys are managed through secure Key Management Services (KMS) with automated rotation and strict access controls.
- Encryption controls and audit logs are reviewed regularly as part of SpruceID's SOC 2 Type II certification process to verify ongoing compliance.

Role-Based Access Control (RBAC)

SpruceID implements granular RBAC to enforce the principle of least privilege across environments. Access is granted strictly by role and limited to the functions necessary for each user's responsibilities.

- Multi-factor authentication (MFA) is required for all administrative access.
- Privilege escalation and system changes are logged and reviewed through continuous monitoring.
- Agency administrators will have configurable control over permissions and audit reporting, ensuring compliance with internal governance and separation-of-duties requirements.

	Summary Through established practices in vulnerability management, encryption, access control, and disaster recovery, SpruceID provides the State of West Virginia with a secure, resilient, and standards-aligned solution. These capabilities are integrated into our operations and verified through independent audit frameworks, ensuring that the One-Stop-Shop Permitting Portal maintains consistent protection and recoverability throughout its lifecycle.

VII.Conclusion

The State of West Virginia's One-Stop-Shop Permitting Program represents a forward-looking commitment to making government services more efficient, transparent, and accessible to all residents. SpruceID's proposed solution directly supports this vision through a secure, user-friendly, and standards-based permitting platform designed to unify processes across agencies while improving the experience for residents and businesses.

Our proposed approach draws on proven implementations in Utah and California, where we have successfully delivered secure, interoperable systems under legislative mandates and complex, multi-agency governance structures. These projects have demonstrated that modernization can be achieved without disruption—by connecting existing systems, automating manual processes, and providing residents with a clear, consistent experience.

SpruceID's solution offers the State:

- A single, streamlined portal for all permitting and licensing activities;
- Configurable workflows that adapt to each agency's operational needs;
- Strong security and compliance through encryption, role-based access, and SOC 2 Type II–audited controls;
- Accessibility and transparency for residents through mobile-friendly design and real-time tracking; and
- A future-ready architecture that will scale as additional agencies and services are added over time.

Throughout this project, SpruceID will remain a collaborative, transparent, and accountable partner—providing full visibility to the State's implementation team, clear service-level commitments, and ongoing support.

By combining modern technology with deep public-sector experience, SpruceID will help West Virginia deliver on its statutory goal under W. Va. Code §5A-13-1 et seq.—creating a One-Stop-Shop Permitting Portal that sets a new standard for digital service delivery, strengthens public trust, and ensures that every West Virginian can access the permits and licenses they need quickly, securely, and confidently.

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		Reason for Modification:
Doc Description:	One-Stop-Shop Permitting Portal -State of West Virginia		
Proc Type:	Central Master Agreement		
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2025-10-24	2025-11-20 13:30	CRFP 0201 SEC2600000001	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000049131
Vendor Name : Spruce Systems, Inc.
Address : 228
Street : Park Avenue S
City : New York
State : New York **Country :** USA **Zip :** 10003
Principal Contact : Wayne Chang
Vendor Contact Phone: +1-917-300-9766☐ **Extension:** n/a

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

Vendor Signature X DocuSigned by: Wayne Chang C4EE4518A56C49F **FEIN#** 85-1064320 **DATE** 11/26/2025

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

ADDITIONAL INFORMATION
REQUEST FOR PROPOSAL

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Department of Administration, Office of the Cabinet Secretary, (hereinafter referred to as the "Agency") to provide a One-Stop-Shop Permitting Portal for the State of West Virginia, per the attached documentation.

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in wvOASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time plus three (3) convenience copies of each to the Purchasing Division. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

INVOICE TO	SHIP TO
SECRETARYS OFFICE BLDG 1 RM E119 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF THE SECRETARY 1900 KANAWHA BLVD E, BLDG 1 RM E119 CHARLESTON WV 25305-0120 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	One-Stop-Shop Permitting Portal -State of West Virginia				

Comm Code	Manufacturer	Specification	Model #
43232408			

Extended Description:
See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. See Section 6, BID SUBMISSION in the CRFP for more information. ********

SCHEDULE OF EVENTS		
Line	Event	Event Date
1	Technical questions due by 3:00 pm	2025-11-03

REQUEST FOR PROPOSAL

CRFP SEC2600000001 - One-Stop-Shop Portal

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION

1.1. Introduction:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code §5A-3-10b, for the WV Department of Administration – Office of Technology, (hereinafter referred to as the "Agency") to provide a One-Stop-Shop Permitting Portal for the State of West Virginia.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

Instructions begin on next page.

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. **REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. **MANDATORY TERMS:** The Solicitation may contain **mandatory** provisions identified by the use of the words "**must**," "**will**," and "**shall**." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. **PRE-BID MEETING:** The item identified below shall apply to this Solicitation.

☑ A pre-bid meeting will not be held prior to bid opening

☐ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the **mandatory** pre-bid meeting. Failure to attend the **mandatory** pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. **VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions **must be submitted on or before the date listed below and to the address listed below to be considered**. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are non-binding.

Submitted emails should have the solicitation number in the subject line. Question Submission Deadline: Monday, November 3, 2025 by 3:00 p.m. EST

Submit Questions to: Tara Lyle, Buyer Supervisor
2019 Washington Street, East Charleston, WV 25305
Fax: (304) 558-3970
Email: Tara.L.Lyle@wv.gov

5. **VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. **BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids or modification of bids via email. Bids submitted by facsimile will be time-stamped as received after all pages have been fully printed. Please ensure facsimiles are started early enough to be delivered in full by the time and date deadline or they will be marked late and will not be evaluated.

Bids submitted in paper, facsimile, or via *wv*OASIS must contain a signature. Failure to submit a bid in any form without a signature will result in rejection of your bid.

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER: Tara Lyle, Buyer Supervisor
SOLICITATION NO.: CRFP SEC2600000001
BID OPENING DATE: November 20, 2025
BID OPENING TIME: 1:30 p.m.
FAX NUMBER: 304-558-3970

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division 2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in *wv*OASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus three (3) convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

7. **BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by *wv*OASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery or via delivery by mail).

Bid Opening Date and Time: November 20, at 1:30 p.m. EST

Bid Opening Location:
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

8. **ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgement Form. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. **BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. **ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand **shall** clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items **may** be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. **COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6.2, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

12. **REGISTRATION:** Prior to Contract award, the apparent successful Vendor **must** be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

13. **UNIT PRICE:** Unit prices **shall** prevail in cases of a discrepancy in the Vendor's bid.

14. **PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15A. **RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15. **WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.7.

16. **ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in *wv*OASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

17. **NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1- 5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance.

18. **ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.6. and § 148-1-6.3.

19. **WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.7. This authority does not apply to instances where state law mandates receipt with the bid.

20. **EMAIL NOTIFICATION OF AWARD:** The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wv*OASIS or the Purchasing Division's website to determine when a contract has been awarded.

21. **EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that **shall** form the basis of a contractual agreement. **Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid.** Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation *may result* in bid disqualification.

SECTION 3: GENERAL TERMS AND CONDITIONS

Terms and conditions begin on next page.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of the Vendor's Offer, creating a Contract by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. ORDER OF PRECEDENCE: This Contract is made up of the following documents, to be construed in the following Order:

2.1. The State's General Terms and Conditions, First Priority

2.2. Any State Addenda or Attachments, Second Priority

2.3. The State's Request for Proposal Document, Third Priority

2.4. Vendor's Bid Response, Fourth Priority

2.5. Any Additional Vendor Documents or Addenda, Fifth Priority

3. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

3.1. "Agency" or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

3.2. "Bid" or **"Proposal"** means the vendors submitted response to this solicitation.

3.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

3.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

3.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

3.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

3.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

3.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

3.9. "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

4. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of Three (3) Years. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to Three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for _____ years;

☐ the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in _____

5. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

6. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☑ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☐ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

7. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

8. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

9. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☑ **Automobile Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☑ **Cyber Liability Insurance** in an amount of: $5,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

10. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

11. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

12. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☑ $10,000 per day for each day the portal fails to be live after Jan. 1, 2027

☐ Liquidated Damages Contained in the Specifications.

☐ Liquidated Damages Are Not Included in this Contract.

13. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

14. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

15. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

16. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

17. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

18. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract and will lead to payment delays and rejection of payment documents. Invoices provided must provide charges and pricing that is consistent with the final Contract.

19. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

20. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials, workmanship, or services provided do not conform to the specifications contained in the Contract. 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.

21. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

22. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

23. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, Office of Technology Policies, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, Office of Technology Policies, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

24. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

25. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

26. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

27. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon, this includes, but is not limited to electronic "click-through" acceptance of Vendor's forms or a third-party's forms.

28. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

29. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

30. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

31. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

32. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

33. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

34. ANTITRUST: In submitting a bid to, signing a contract with, or accepting an Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

35. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

36. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

37. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

38. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

39. CONFLICT OF INTEREST: Vendor, its officers, members, or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members, and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

40. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☑ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc. Any reports identified in the specifications.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

41. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

42. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

47. DISENTANGLEMENT CLAUSE: The purpose of this provision is to ensure an orderly, efficient, and secure transition of services, data, and responsibilities from the Contractor to the State or a successor service provider at the expiration or termination of this Agreement, without disruption to State operations. Upon notice of termination or expiration of this Agreement, the Contractor shall fully cooperate with the State and any successor contractor to ensure a smooth transition. The Contractor shall provide all reasonable assistance requested by the State, including but not limited to:

- Transition planning and coordination meetings;
- Delivery of current documentation, system configurations, inventories, and as-built diagrams in a format mutually agreed to between the State and the Contractor;
- Continuation of services during the transition period; and
- Transfer of operational knowledge and best practices.

The Contractor shall continue providing services, at the same level of quality and responsiveness, for a transition period designated by the State, if necessary, not to exceed 6 months following termination or expiration, unless otherwise agreed to in writing. The State shall compensate the Contractor for such continued services at the rates specified in this Agreement. Within 30 days of contract termination or expiration, the Contractor shall return to the State all State data, including backups, metadata, and configurations, in a mutually agreed, machine-readable format. The Contractor shall certify in writing that all State data has been permanently deleted from Contractor and subcontractor systems in accordance with State-approved data destruction policies.

All deliverables, configurations, system documentation, runbooks, and other materials developed or used to perform the contracted services that are necessary for the continued operation of the system shall be delivered to the State. The Contractor shall not withhold or restrict access to such materials for any reason, including the existence of disputes or unpaid invoices. The Contractor shall provide the State and any successor contractor with reasonable access to personnel, systems, facilities, and documentation as needed to perform transition activities. The Contractor shall ensure that all subcontractors comply with these same requirements.

The Contractor shall ensure that there is no degradation or interruption of services during the transition period. Any failure to maintain service levels during the transition shall be considered a material breach of contract.

Within 90 days of contract execution, the Contractor shall provide a draft Disentanglement and Transition Plan for State approval. The plan shall describe processes, timelines, roles, and resources necessary to transition services with minimal disruption.

The Contractor shall bear all costs associated with meeting its disentanglement obligations unless otherwise specified. Costs for optional transition support beyond the defined scope may be negotiated at the State's discretion.

The Contractor shall coordinate with the State to maintain continuity of operations throughout the transition, including compliance with all security, privacy, and regulatory requirements until all State data and operations are fully transitioned.

The Contractor shall provide data export utilities, schema documentation, and API access to facilitate migration to another provider. All data formats and interfaces must remain accessible and documented through the end of the transition period.

48. SUBCONTRACTOR LIST SUBMISSION: For the purposes of Information Technology Contracts, the Vendor must provide a list of Subcontractors that the Vendor intends to utilize in order to fulfill this Contract. Any Subcontractor or entity outside of the Vendor who will be performing work under this Contract or will have access to any State data, information, or the State network during the performance of this Contract must be submitted prior to Contract Award. This list will be provided to the West Virginia Office of Technology for review and approval prior to Contract execution to confirm the State's security needs. The Office of Technology reserves the right to reject any proposed Subcontractors on this list, and to provide a cancellation request to the Purchasing Division and the Agency regarding any cybersecurity, privacy, or other Office of Technology policy concerns that are unable to be addressed by the Vendor.

a. Required Information. The subcontractor list must contain the following information:

i. Bidder's name
ii. Name of each subcontractor
iii. Identification of the work each subcontractor will provide toward the project and/or access they will be granted during this project.
iv. Any additional information which would assist the WV Office of Technology in evaluating the Subcontractor

b. Subcontractor List Submission Form: The subcontractor list may be submitted in any form, including the attached form, as long as the required information noted above is included. If any information is missing from the bidder's subcontractor list submission, it may be obtained from other documents such as bids, emails, letters, etc. that accompany the subcontractor list submission.

Subcontractor List Submission (Information Technology)

Bidder's Name: Spruce Systems, Inc.

☒ 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

Attach additional pages if necessary

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) Wayne Chang CEO

(Address) 228 Park Avenue S, New York, NY 10003

(Phone Number) / (Fax Number) +1-917-300-9766☐

(email address) wayne@spruceid.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.

Spruce Systems, Inc.
(Company)

DocuSigned by:
Wayne Chang
C45F4518A56C09A...
(Signature of Authorized Representative)

Wayne Chang CEO 11/26/2025
(Printed Name and Title of Authorized Representative) (Date)

+1-917-300-9766☐ Fax: n/a
(Phone Number) (Fax Number)

wayne@spruceid.com
(Email Address)

REQUEST FOR PROPOSAL
CRFP SEC2600000001 - One-Stop-Shop Portal

SECTION 4: PROJECT SPECIFICATIONS

4.1.Background and Current Operating Environment: This project will create a portal for West Virginia's One Stop Shop Permitting Program, as described in House Bill 2002, passed during the 2025 Legislative Session. This portal should provide a public-facing dashboard where those wishing to do business in the State can go to identify and apply for the necessary permits, licenses, and other approvals needed to start and maintain business opportunities within the State. Per the Enacting Statute, WV Code §5A-13-1 et seq., this program must incorporate and include the permitting, licensing, and approvals of the following agencies currently:

- The Department of Commerce;
- The Department of Environmental Protection;
- The Office of Environmental Health Services;
- The Department of Revenue, except the Lottery, Lottery Commission, and the Division of Financial Institutions;
- The Department of Tourism, The Department of Transportation, except the Division of Motor Vehicles; and
- The Secretary of State.

4.2.Project Goals and Mandatory Requirements: The intent of this program is to revolutionize and streamline West Virginia's permitting system by creating an online dashboard for processing and tracking permits for construction, economic development, infrastructure, and natural resource projects. The goal of this solicitation is to acquire a contract for the development, creation, and implementation of a permitting portal system, that will facilitate the intent of the program through effective workflows and user-friendly access to permitting information, applications, and tracking.

The State requires a solution that 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 solution must be flexible and scalable to adapt to increased requirements in future years.

West Virginia needs a solution in this area that is dynamic, capable of managing the permitting process and streamlining workflows, but also flexible, customizable, and expandable to encompass additional agencies and permits as necessary in the future. Vendor should describe its approach and methodology to provide the service or solve the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

4.2.1. Goals and Objectives – The project goals and objectives are listed below.

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.

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

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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

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-13-1 et seq., which mandates full implementation of the One-Stop-Shop Permitting Program by **January 1, 2027.**

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.

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.

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.

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.

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.

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

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

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.

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.

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

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.

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.

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.

4.2.2.4 Vendor's proposed solution must meet FedRAMP requirements.

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

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.

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

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.

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.

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.

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.

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

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

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

4.2.2.15 Vendor must provide 3-tier outage reporting.

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.

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.

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.

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.

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.

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

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

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.

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.

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.

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

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

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.

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

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

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).

4.4. Oral Presentations (Agency Option): The Agency has the option of requiring oral presentations of all Vendors participating in the RFP process. If this option is exercised, points will be allocated in Section 6.2 below at the time the RFP is issued, or via addendum prior to technical bid opening. During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:

Materials and Information Requested at Oral Presentation:

4.4.1. Virtual presentation to committee outlining proposal, methodology, and providing an informal project demo.

SECTION 5: VENDOR PROPOSAL

5.1. Economy of Preparation: Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

5.2. Incurring Cost: Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

5.3. Proposal Format: Vendors should provide responses in the format listed below:

5.3.1. **Two-Part Submission:** Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

5.3.2. **Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

5.3.3. **Table of Contents:** Clearly identify the material by section and page number.

5.3.4. **Response Reference:** Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

Proposal Submission: All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

SECTION 6: EVALUATION AND AWARD

6.1. Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

6.2. Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

Evaluation Point Allocation:

Project Goals and Proposed Approach (§ 4.2)	
- Approach & Methodology to Goals/Objectives (§ 4.2.1)	25 Points Possible
- Approach & Methodology to Compliance with Mandatory Project Requirements (§ 4.2.2)	15 Points Possible
Qualifications and experience (§ 4.3)	
- Qualifications and Experience Generally (§ 4.3.1)	10 Points Possible
- Exceeding Mandatory Qualification/Experience Requirements (§ 4.3.2)	5 Points Possible
(Oral interview, if applicable) (§ 4.4)	15 Points Possible
Total Technical Score:	70 Points Possible
Total Cost Score:	30 Points Possible
Total Proposal Score:	**100 Points Possible**

REQUEST FOR PROPOSAL

CRFP SEC2600000001 - One-Stop-Shop Portal

6.3. Technical Bid Opening: At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

6.4. Technical Evaluation: The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

6.5. Proposal Disqualification:

6.5.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

6.6. Cost Bid Opening: The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

6.7. Cost Evaluation: The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

REQUEST FOR PROPOSAL
CRFP SEC2600000001 - One-Stop-Shop Portal

Example:

Proposal 1 Cost is $1,000,000
Proposal 2 Cost is $1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Spruce Systems, Inc.

(Company)

Wayne Chang CEO

(Representative Name, Title)

+1-917-300-9766☐ Fax: n/a

(Contact Phone/Fax Number)

11/26/2025

(Date)

REQUEST FOR PROPOSAL

CRFP SEC2600000001 - One-Stop-Shop Portal

Attachment A: Cost Sheet

CRFP SEC2600000001
Cost Sheet - Attachment A

Category	Description	Unit/Qty	Rate	Total Cost
Implementation Fee	One-time setup, configuration, onboarding, and training	1		
Annual License Fee	Recurring license for platform usage	1 year		
Maintenance	System updates, and ongoing maintenance	1 year		
Unlimited Users	Platform access for unlimited internal/external users	Included		
Customer Support	Email/chat support, knowledge base, ticketing system	1 year		
Call Center Support	Dedicated phone support for agencies and public inquiries	1 year		
Internal Users	Staff/admin access across agencies	500	Included	
External Users	Public-facing portal for applicants, businesses, and citizens	Unlimited	Included	
Data Migration	Import of legacy digital data into new system	At least one agency will require full digital transition	$X.XX/GB	
Paper to Digital Migration	Scanning, digitization, and indexing of paper records		$X.XX/unit	

Optional Add-Ons

Add-On	Description	Rate	Total Cost
Agency Expansion	Support for onboarding additional agencies beyond initial 9	$X,.XX/agency	
Onboarding Additional Agencies	API connections to third-party systems (e.g., CRM, payment gateways)	$X.XX/system	
Creating additional custom workflows	Automated alerts for users and admins	$X.XX/year	
License/Permit Types	Configuration of multiple license/permit workflows in addition to initial setup	$X.XX/type	
E-Signature Integration	Digital signatures for applications and approvals	$X.XX/year	
Storage	Storage of documents and Hosting of System, should the State elect not to transition to its own cloud storage	$X.XX/TB/year	

Suggested Payment Schedule

Milestone	% of Total	Due Upon
Contract Signing & Kickoff	10%	After Kick-Off Meeting and Deliverable Schedule Presented and Agreed to by both parties
Completion of System Configuration	25%	After configuration and initial testing
Data Migration & Agency Onboarding	25%	After successful migration and agency setup
Go-Live & User Training	20%	Upon go-live and completion of training
Final Acceptance & Warranty Start	20%	30 days post go-live, after issue resolution

Vendor Name _____ Authorized Siganture _____ Date _____