Procurement   Budgeting   Accounts Receivable   Accounts Payable

Welcome, Christopher W Sackman

Solicitation Response(SR) Dept: 0231 ID: ES0030325000000915325 Ver.: 1 Function: New Phase: Final   Modified by Sackman, 03/07/2025

Header # 1

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 1619976

Procurement Type: Central Contract - Fixed Amt

Vendor ID: VS0000046894

Legal Name: LSP Data Solutions, LLC

Alias/DBA: LSP Data Solutions, LLC

Total Bid: $67,300.00

Response Date: 03/06/2025

Response Time: 14:44

Responded By User ID: 56210

First Name: Kane

Last Name: Jones

Email: kjones@lspdata.com

Phone: 8049958467

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: DOT2500000017

Published Date: 3/3/25

Close Date: 3/7/25

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No 2 Cybersecurity e-Discovery SAAS (DT25)Y2

Total of Header Attachments: 3

Total of All Attachments: 3

	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Solicitation Response

Proc Folder:	1619676
Solicitation Description:	Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112
Proc Type:	Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2025-03-07 13:30	SR 0231 ESR03032500000005320	1

VENDOR
VS0000046084 LSP Data Solutions, LLC

Solicitation Number:	CRFQ 0231 OOT2500000017

Total Bid:	67300	**Response Date:**	2025-03-06	**Response Time:**	14:44:36

Comments:

Vendor **Signature X**   **FEIN#**   **DATE**

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Contract Services: e-Discovery System				67300.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Commodity Line Comments:

Extended Description:

Please see the attached Exhibit A Pricing Page
Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

Proc Folder: 1619676	**Reason for Modification:**
Doc Description: Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112	Addendum no 2 is issued to publish questions and answers and to modify the bid opening date.
Proc Type: Central Contract - Fixed Amt	

Date Issued	Solicitation Closes	Solicitation No	Version
2025-03-03	2025-03-07 13:30	CRFQ 0231 OOT2500000017	3

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON   WV   25305

US

VENDOR

Vendor Customer Code:

Vendor Name : LSP Data Solutions LLC

Address :

Street : 1101 14th St NW, Suite 750

City : Washington

State : DC   **Country :** USA   **Zip :** 20005

Principal Contact : Robert Chuey, Managing Partner

Vendor Contact Phone: 202-924-1663   **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X *Robert Chuey*   **FEIN#** 81-142-0652   **DATE** 03/04/2025

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

ADDITIONAL INFORMATION

Addendum No 2 is issued for the following reasons:

1) To Publish Vendor questions with the Agency's responses.

2) To modify the bid opening date from 3/5/25 to 3/7/25.

--no other changes--

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Contract Services: e-Discovery System				

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description:
Please see the attached Exhibit A Pricing Page

Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2025-02-18

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

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: Tuesday February 18, 2025 @3:00 p.m

Submit Questions to: Toby L Welch
2019 Washington Street, East Charleston, WV 25305
Fax: (304) 558-3970
Email: Toby.L.Welch@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 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: Toby L Welch
SOLICITATION NO.: CRFQ OOT2500000017
BID OPENING DATE: Wednesday February 26, 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

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: 02/26/25 @ 1:30 p.m.

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. **SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:**
For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority- owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors.

16. **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.

17. **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.

18. **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."

19. **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."

20. **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.

21. **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.

22. **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.

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 this Contract made 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. 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.

2.1. "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.

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

2.3. "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.

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

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

2.6. "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.

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

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

2.9. "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.

3. 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 ‎One (1) Year‎ _____. 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 _____

4. 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.

5. 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.

6. 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.

7. 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.

WV Software as a Service Addendum Attached as Appendix A. See specification 4.1.10

☑

☐

☐

☐

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.

8. 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: _____ 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: $1,000,000.00 _____ 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.

☐

☐

☐

☐

9. 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.

10. 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.

11. 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:

☐ _____ for _____ .

☐ Liquidated Damages Contained in the Specifications.

☑ Liquidated Damages Are Not Included in this Contract.

12. 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.

13. 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.

14. 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.

15. 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.)

16. 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.

17. 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.

18. 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.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied 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.

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

21. 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.

22. 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, 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, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. CONFLICT OF INTEREST: Vendor, its officers or 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.

39. 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.

☐ 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.

40. 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.

41. 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. As used in this section:

    a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

    b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

    c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

        1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

        2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

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.

ADDITIONAL TERMS AND CONDITIONS (Construction Contracts Only)

1. CONTRACTOR'S LICENSE: Until June 15, 2021, West Virginia Code § 21-11-2, and after that date, § 30-42-2, requires that all persons desiring to perform contracting work in this state be licensed. The West Virginia Contractors Licensing Board is empowered to issue the contractor's license. Applications for a contractor's license may be made by contacting the West Virginia Contractor Licensing Board.

The apparent successful Vendor must furnish a copy of its contractor's license prior to the issuance of a contract award document.

2. BONDS: The following bonds must be submitted:

☐ **BID BOND:** Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. **THE BID BOND MUST BE SUBMITTED WITH THE BID OR VENDOR'S BID WILL BE DISQUALIFIED.**

☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)

☐ **LABOR/MATERIAL PAYMENT BOND**: The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)

☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system if the work impacts an existing roof. The amount of the bond must be equal to the price associated with the percentage of the project impacting the roof. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)

At a minimum, all construction projects require a bid bond, performance bond, and labor/material payment bond. Failure on the part of the state of West Virginia to checkmark the required bonds above does not relieve the vendor from the legal requirement of providing these bonds.

In lieu of the Bid Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of the bid bond must be of the same amount required of the Bid Bond and delivered with the bid.

3. DRUG-FREE WORKPLACE AFFIDAVIT: W. Va. Code § 21-1D-5 provides that any solicitation for a public improvement contract requires each Vendor that submits a bid for the work to submit an affidavit that the Vendor has a written plan for a drug-free workplace policy. If the affidavit is not submitted with the bid submission, the Purchasing Division shall promptly request by telephone and electronic mail that the low bidder and second low bidder provide the affidavit within one business day of the request. Failure to submit the affidavit within one business day of receiving the request shall result in disqualification of the bid. To comply with this law, Vendor should complete the enclosed drug-free workplace affidavit and submit the same with its bid. Failure to submit the signed and notarized drugfree workplace affidavit or a similar affidavit that fully complies with the requirements of the applicable code, within one business day of being requested to do so shall result in disqualification of Vendor's bid. Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is $100,000 or less or temporary or emergency repairs.

3.1. DRUG-FREE WORKPLACE POLICY: Pursuant to W. Va. Code § 21-1D-4, Vendor and its subcontractors must implement and maintain a written drug-free workplace policy that complies with said article. The awarding public authority shall cancel this contract if: (1) Vendor fails to implement and maintain a written drug-free workplace policy described in the preceding paragraph, (2) Vendor fails to provide information regarding implementation of its drug-free workplace policy at the request of the public authority; or (3) Vendor provides to the public authority false information regarding the contractor's drug-free workplace policy.

Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is $100,000 or less or temporary or emergency repairs.

4. DRUG FREE WORKPLACE REPORT: Pursuant to W. Va. Code § 21-1D-7b, no less than once per year, or upon completion of the project, every contractor shall provide a certified report to the public authority which let the contract. For contracts over $25,000, the public authority shall be the West Virginia Purchasing Division. For contracts of $25,000 or less, the public authority shall be the agency issuing the contract. The report shall include:

(1) Information to show that the education and training service to the requirements of West Virginia Code § 21-1D-5 was provided;

(2) The name of the laboratory certified by the United States Department of Health and Human Services or its successor that performs the drug tests;

(3) The average number of employees in connection with the construction on the public improvement;

(4) Drug test results for the following categories including the number of positive tests and the number of negative tests: (A) Pre-employment and new hires; (B) Reasonable suspicion; (C) Post-accident; and (D) Random.

Vendor should utilize the attached Certified Drug Free Workplace Report Coversheet when submitting the report required hereunder. Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is $100,000 or less or temporary or emergency repairs.

Revised 8/24/2023

5. AIA DOCUMENTS: All construction contracts that will be completed in conjunction with architectural services procured under Chapter 5G of the West Virginia Code will be governed by the attached AIA documents, as amended by the Supplementary Conditions for the State of West Virginia, in addition to the terms and conditions contained herein.

6. PROHIBITION AGAINST GENERAL CONDITIONS: Notwithstanding anything contained in the AIA Documents or the Supplementary Conditions, the State of West Virginia will not pay for general conditions, or winter conditions, or any other condition representing a delay in the contracts. The Vendor is expected to mitigate delay costs to the greatest extent possible and any costs associated with Delays must be specifically and concretely identified. The state will not consider an average daily rate multiplied by the number of days extended to be an acceptable charge.

7. GREEN BUILDINGS MINIMUM ENERGY STANDARDS: In accordance with § 22-29-4, all new building construction projects of public agencies that have not entered the schematic design phase prior to July 1, 2012, or any building construction project receiving state grant funds and appropriations, including public schools, that have not entered the schematic design phase prior to July 1, 2012, shall be designed and constructed complying with the ICC International Energy Conservation Code, adopted by the State Fire Commission, and the ANSI/ASHRAE/IESNA Standard 90.1-2007: Provided, That if any construction project has a commitment of federal funds to pay for a portion of such project, this provision shall only apply to the extent such standards are consistent with the federal standards.

8. LOCAL LABOR MARKET HIRING REQUIREMENT: Pursuant to West Virginia Code §21-1C-1 et seq., Employers shall hire at least seventy-five percent of employees for public improvement construction projects from the local labor market, to be rounded off, with at least two employees from outside the local labor market permissible for each employer per project.

Any employer unable to employ the minimum number of employees from the local labor market shall inform the nearest office of Workforce West Virginia of the number of qualified employees needed and provide a job description of the positions to be filled.

If, within three business days following the placing of a job order, Workforce West Virginia is unable to refer any qualified job applicants to the employer or refers less qualified job applicants than the number requested, then Workforce West Virginia shall issue a waiver to the employer stating the unavailability of applicant and shall permit the employer to fill any positions covered by the waiver from outside the local labor market. The waiver shall be in writing and shall be issued within the prescribed three days. A waiver certificate shall be sent to both the employer for its permanent project records and to the public authority.

Any employer who violates this requirement is subject to a civil penalty of $250 per each employee less than the required threshold of seventy-five percent per day of violation after receipt of a notice of violation.

Any employer that continues to violate any provision of this article more than fourteen calendar days after receipt of a notice of violation is subject to a civil penalty of $500 per each employee less than the required threshold of seventy-five percent per day of violation.

The following terms used in this section have the meaning shown below.

(1) The term "construction project" means any construction, reconstruction, improvement, enlargement, painting, decorating or repair of any public improvement let to contract in an amount equal to or greater than $500,000. The term "construction project" does not include temporary or emergency repairs;

(2) The term "employee" means any person hired or permitted to perform hourly work for wages by a person, firm or corporation in the construction industry; The term "employee" does not include:(i) Bona fide employees of a public authority or individuals engaged in making temporary or emergency repairs;(ii) Bona fide independent contractors; or(iii) Salaried supervisory personnel necessary to assure efficient execution of the employee's work;

(3) The term "employer" means any person, firm or corporation employing one or more employees on any public improvement and includes all contractors and subcontractors;

(4) The term "local labor market" means every county in West Virginia and any county outside of West Virginia if any portion of that county is within fifty miles of the border of West Virginia;

(5) The term "public improvement" includes the construction of all buildings, roads, highways, bridges, streets, alleys, sewers, ditches, sewage disposal plants, waterworks, airports and all other structures that may be let to contract by a public authority, excluding improvements funded, in whole or in part, by federal funds.

9. DAVIS-BACON AND RELATED ACT WAGE RATES:

☐ The work performed under this contract is federally funded in whole, or in part. Pursuant to

_____, Vendors are required to pay applicable Davis-Bacon wage rates.

☐ The work performed under this contract is not subject to Davis-Bacon wage rates.

10. SUBCONTRACTOR LIST SUBMISSION: In accordance with W. Va. Code § 5-22-1, the apparent low bidder on a contract valued at more than $250,000.00 for the construction, alteration, decoration, painting or improvement of a new or existing building or structure shall submit a list of all subcontractors who will perform more than $25,000.00 of work on the project including labor and materials. (This section does not apply to any other construction projects, such as highway, mine reclamation, water or sewer projects.) The subcontractor list shall be provided to the Purchasing Division within one business day of the opening of bids for review.
If the apparent low bidder fails to submit the subcontractor list, the Purchasing Division shall promptly request by telephone and electronic mail that the low bidder and second low bidder provide the subcontractor list within one business day of the request. Failure to submit the subcontractor list within one business day of receiving the request shall result in disqualification of the bid.

If no subcontractors who will perform more than $25,000.00 of work are to be used to complete the project, the apparent low bidder must make this clear on the subcontractor list, in the bid itself, or in response to the Purchasing Division's request for the subcontractor list.

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

        i. Bidder's name

        ii. Name of each subcontractor performing more than $25,000 of work on the project.

        iii. The license number of each subcontractor, as required by W. Va. Code § 21-11-1 et. seq.

        iv. If applicable, a notation that no subcontractor will be used to perform more than $25,000.00 of work. (This item iv. is not required if the vendor makes this clear in the bid itself or in documentation following the request for the subcontractor list.)

    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.

    c. Substitution of Subcontractor. Written approval must be obtained from the State Spending Unit before any subcontractor substitution is permitted. Substitutions are not permitted unless:

        i. The subcontractor listed in the original bid has filed for bankruptcy;

        ii. The subcontractor in the original bid has been debarred or suspended; or

        iii. The contractor certifies in writing that the subcontractor listed in the original bid fails, is unable, or refuses to perform his subcontract.

Subcontractor List Submission (Construction Contracts Only)

Bidder's Name: ___LSP Data Solutions LLC___

☑ Check this box if no subcontractors will perform more than $25,000.00 of work to complete the project.

Subcontractor Name	License Number if Required by W. Va. Code § 21-11-1 et. seq.

Attach additional pages if necessary

ADDITIONAL TERMS AND CONDITIONS
(Architectural and Engineering Contracts Only)

1. PLAN AND DRAWING DISTRIBUTION: All plans and drawings must be completed and available for distribution at least five business days prior to a scheduled pre-bid meeting for the construction or other work related to the plans and drawings.

2. PROJECT ADDENDA REQUIREMENTS: The Architect/Engineer and/or Agency shall be required to abide by the following schedule in issuing construction project addenda. The Architect/Engineer shall prepare any addendum materials for which it is responsible, and a list of all vendors that have obtained drawings and specifications for the project. The Architect/Engineer shall then send a copy of the addendum materials and the list of vendors to the State Agency for which the contract is issued to allow the Agency to make any necessary modifications. The addendum and list shall then be forwarded to the Purchasing Division buyer by the Agency. The Purchasing Division buyer shall send the addendum to all interested vendors and, if necessary, extend the bid opening date. Any addendum should be received by the Purchasing Division at least fourteen (14) days prior to the bid opening date.

3. PRE-BID MEETING RESPONSIBILITIES: The Architect/Engineer shall be available to attend any pre-bid meeting for the construction or other work resulting from the plans, drawings, or specifications prepared by the Architect/Engineer.

4. AIA DOCUMENTS: All construction contracts that will be completed in conjunction with architectural services procured under Chapter 5G of the West Virginia Code will be governed by the attached AIA documents, as amended by the Supplementary Conditions for the State of West Virginia, in addition to the terms and conditions contained herein. The terms and conditions of this document shall prevail over anything contained in the AIA Documents or the Supplementary Conditions.

5. GREEN BUILDINGS MINIMUM ENERGY STANDARDS: In accordance with West Virginia Code § 22-29-4, all new building construction projects of public agencies that have not entered the schematic design phase prior to July 1, 2012, or any building construction project receiving state grant funds and appropriations, including public schools, that have not entered the schematic design phase prior to July1, 2012, shall be designed and constructed complying with the ICC International Energy Conservation Code, adopted by the State Fire Commission, and the ANSI/ASHRAE/IESNA Standard 90.1-2007: Provided, That if any construction project has a commitment of federal funds to pay for a portion of such project, this provision shall only apply to the extent such standards are consistent with the federal standards.

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) _Karen Jones, Contracts Manager_

(Address) _1101 14th St NW, Suite 750 Washington D.C. 20005_

(Phone Number) / (Fax Number) _804-750-5913_

(email address) _kjones@lspdata.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 an 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.

LSP Data Solutions LLC

(Company)

Robert Chuey

(Signature of Authorized Representative)

Robert Chuey, Managing Partner   03/04/2025

(Printed Name and Title of Authorized Representative) (Date)

202-924-1663

(Phone Number) (Fax Number)

rchuey@lspdata.com

(Email Address)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.:

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

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

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

☑ Addendum No. 1   ☐ Addendum No. 6
☑ Addendum No. 2   ☐ Addendum No. 7
☐ Addendum No. 3   ☐ Addendum No. 8
☐ Addendum No. 4   ☐ Addendum No. 9
☐ Addendum No. 5   ☐ Addendum No. 10

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

LSP Data Solutions LLC
_____
Company

Robert Chrey
_____
Authorized Signature

03/04/2025
_____
Date

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

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for an e-Discovery software as a service. This software will be used for discovery in legal proceedings to process emails and other files. The software will facilitate keyword searching, document review, privilege report creation, data tagging and redaction prior to final report being released.

   WVOT provides highly reliable, protected, and cost-effective technology services to approximately 25,000 computers and 20,000 network users. Services are delivered by approximately 200 full-time and temporary employees and supplemented by specialized contract services and staff on an as-needed basis. There are approximately 210 entities total within the executive branch where services are provided. Funding for the Office of Technology is derived from a fee for services model.

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

   2.1 "Business Hours" means Monday - Friday 8:00 AM to 5:00 PM EST excluding weekends and Federal and State holidays, which are as follows:
   - **2.1.1** New Year's Day (January 1)
   - **2.1.2** Martin Luther King Day (Third Monday in January)
   - **2.1.3** President's Day (Third Monday in February)
   - **2.1.4** Memorial Day (Last Monday in May)
   - **2.1.5** West Virginia Day (June 20)
   - **2.1.6** Independence Day (July 4)
   - **2.1.7** Labor Day (First Monday in September)
   - **2.1.8** Columbus Day (Second Monday in October)
   - **2.1.9** Veterans Day (November 11)
   - **2.1.10** Thanksgiving (Fourth Thursday in November)
   - **2.1.11** Day After Thanksgiving (Fourth Friday in November)
   - **2.1.12** Christmas Day (December 25)

   2.2 "Contract Services" means an e-Discovery system as more fully described in these specifications.

   2.3 "Pricing Page" means the pages, contained wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the Contract Services.

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

3. **QUALIFICATIONS:** Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1.   The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section AC-17 Remote Access, and Section 3.3.1. Cloud Computing.

4. MANDATORY REQUIREMENTS:

4.1 Mandatory Contract Services Requirements and Deliverables: Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1   General Requirements– e-Discovery System

4.1.1.1 The Vendor must provide an e-Discovery System that is cloud-based (Software as a Service Model). as well as support Automated Cloud Data Collections and Connectors

4.1.1.2 The system must contain the following capabilities within a single platform that does not require integration with other software: self-service data loading, self-service data processing, client administration, self-service, productions, review, and analytics capabilities.

4.1.1.3 The Vendor must provide an e-Discovery System with unlimited user seats for a minimum of 12 months from date of award.

4.1.1.4 The system must allow client administrators to have the ability to set-up new users or workspaces and assign roles and permissions to new users.

4.1.1.5 The system must allow a user to have multiple roles and toggle between roles. For example, a client administrator can toggle between user roles to validate user permissions and provide user support.

4.1.1.6 The system must not require additional licenses and/or software from third parties.

4.1.1.7 The system must allow the customer/client administrators the ability to remove/delete documents and create archives from the platform.

4.1.1.8 The system must be accessible to an unlimited number of users and allow access to at least 50 concurrent cases each having at least one million documents without degradation to speed.

4.1.1.9 The system must be a configurable Platform that allows the administrators to configure applications like request tracking and FOIA requests.

4.1.1.10 The system must be built on scalable architecture with a storage capacity of at least two petabytes of data.

4.1.1.11 The Vendor must provide an e-Discovery System that features the following:

4.1.1.11.1 A system that has two-factor authentication access.

4.1.1.11.2 A system that allows the Agency to have 100% data input automation. The Vendor must not have access to Agency-owned data.

4.1.1.11.3 A system that provides 256-bit encryption to the data when at rest and in transit.

4.1.1.11.4 A system that scans files for viruses.

4.1.1.11.5 A system that allows for load file import and export.

4.1.2 Data Loading & Processing- e-Discovery System

4.1.2.1 The system must allow the Agency to have 100% data input automation.

4.1.2.2 The system must allow the user to load raw data such as PSTs, zip files, and other ESI for processing.

4.1.2.3 The system must allow the client administrator to move data between data stores and conduct early case assessment, including running search terms, and listing and counting file types reports, prior to making the data available to reviewers.

4.1.2.4 The system must allow the customer to create, save, and upload templates for data processing.

4.1.2.5 The system must have pre-built utilities to support processing for various files including imaging, loading, and text files.

4.1.2.6 The system must support uploading up to 10 GB of data directly from web-browser via "drag and drop".

4.1.2.7 The system must allow loading and processing of a data set that has at least 1 terabyte of documents, data, or ESI, into the review tool.

4.1.2.8 The system must support data reduction and culling (De-NIST; custodial and global Deduplication; filtering by Custodian, file type, date; keyword searching) during processing.

4.1.2.9 The system must include built-in ESI processing capabilities (extraction of text and metadata, imaging, numbering, OCR, load file creation).

4.1.2.10 The system must keep emails and families together and locate orphaned documents during processing.

4.1.2.11 The system must support extraction and processing of files within container files such as zip and rar, and support the processing of files in nested containers or folders.

4.1.2.12 The system must have the ability to ingest, process, and view multiple file types.

4.1.2.13 The system must allow for load file import and export.

4.1.2.14 The system must allow the user the ability to create templates for processing, production, import, export.

4.1.2.15 The system must be able to securely transfer ESI to the review tool.

4.1.3 Review – e-Discovery System

4:1.3.1 The system must allow users to review and analyze ESI productions.

4.1.3.2 The system must allow users to identify and remove duplicate documents and data.

4.1.3.3 The system must allow users to redact and highlight portions of the document.

4.1.3.4 The system must allow users to search, tag, index, and code information and provide advance search features including but not limited to keyword, Boolean, stemming, wildcard, fuzzy, proximity and other search types.

4.1.3.5 The system must process searches, display documents, and allow users to perform document review with minimal loading times.

4.1.3.6 The system must include a file viewer that easily and quickly opens files without needing to install additional applications. Supported files must include: .docx, .xlsx, .pdf, .jpg, .jpeg, .mov, avi, .rtf, .txt., pub, .pptx.

4.1.3.7 The system must support searching on tags/codes and metadata.

4.1.3.8 The system must allow the user the option to assign and self-assign batches for review.

4.1.3.9 The system must provide search engines that support both Elasticsearch and dtSearch indexing and searching options within a single matter.

4.1.3.10 The system must allow the user to create workspaces, folders, etc., for customizable document organization.

4.1.3.11 The system must provide full administrator rights to the customer, including the ability to assign roles/permissions, create review assignments and/ or review batches for reviewers.

4.1.3.12 The system must allow for the customization of coding panels.

4.1.4 Advanced Analytics – eDiscovery System

4.1.4.1 The system must include the following content & context analysis capabilities: topic clustering, email threading, near-duplicate analysis, entities recognition.

4.1.4.2 The system must provide predictive coding, advanced artificial intelligence (AI) and Technology Assisted Review (TAR) technologies including TAR 1.0 and TAR 3.0.

4.1.4.3 The system must provide Active Learning (story builder with continuous active learning analytics).

4.1.5 Security – eDiscovery System

4.1.5.1 The system must provide secure authorized access and have multi-factor authentication for each user to prevent unauthorized access.

4.1.5.2 The systems must provide automatic session termination if no activity with a prescribed period of time.

4.1.5.3 The system must allow a client administrator to restrict security rights at the individual, group or role level.

4.1.5.4 The system must provide a security level that allows system administrators to add new users to the system and edit existing user permissions.

4.1.5.5 The vendor must provide regular maintenance including new releases and updates.

4.1.5.6 The system must provide at least 256-bit encryption to the data when at rest and in transit.

4.1.6 Production – eDiscovery System

4.1.6.1 The system must provide production of the ESI in a variety of formats including as searchable PDF, native or images and text with a load file.

4.1.6.2 The system must have a wizard-driven production process.

4.1.6.3 The system must have self-service production capabilities to allow the user to prepare and export from start to finish/download.

4.1.6.4 The system must allow the user to view all productions for a single file in the review platform.

4.1.7 Professional Services and Training – eDiscovery

4.1.7.1 The vendor must provide live training (which may be virtual).

4.1.7.2 The vendor must provide reviewer training and client administrator/organization administrator training.

4.1.7.3 The vendor must record live training and provide recorded training to the client at no additional cost.

4.1.7.4 The system must provide access to a knowledge base or help center, technical documentation, and online support resources.

4.1.7.5 The vendor must provide support services for the initial setup.

4.1.7.6 The vendor must provide support services for the duration of the contract for ongoing maintenance.

4.1.7.7 The vendor must offer client services support including project management and technical support services.

4.1.8 Support - eDiscovery

4.1.8.1 Support by telephone, online, in-app, and email 24 hours-a-day, 7 days-a-week, 365 days-a-year for troubleshooting technical issues

4.1.8.2 A response time of a minimum of 1 day to request for technical support.

4.1.8.3 Access to knowledgebase, technical documentation, and online support resources.

4.1.9 Billing - eDiscovery

4.1.9.1 Vendor will round up to the nearest next whole gigabyte (GB) for billing and auditing purposes. (Example 1.2GB will be billed at 2.0 GB)

4.1.9.2 Vendor will invoice monthly and bill at the maximum gigabyte (GB) capacity used by the state.

4.1.9.3 Vendor's proposed solution must provide billing capabilities designed to simplify the procedures of a chargeback model, as well as provide a holistic view of service. The state desires the billing detail to include but not be limited to billing by agency, consumption usage by each agency.

4.1.10 Software as a Service Addendum

4.1.10.1 Vendor must sign the attached Software as a Service Addendum prior to award.

4.1.11 Optional Renewals

4.1.11.1 Vendor will include in their bid the cost of optional Annual renewals for years 2, 3, and 4. These optional Annual renewals will be initiated on Agency request authorized under the authority of the Purchasing Division.

5 CONTRACT AWARD:

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the

Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

5.2 Contract will be evaluated on all lines but only awarded for the first year with the option for renewal at the end of the first-year term. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

5.3 Pricing Page: Vendor should complete the attached Exhibit A - Pricing Page by providing the unit cost per Gigabyte (GB) per month. The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line 1. The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

5.3.1 The Pricing Page contains a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

5.3.2 Vendor should provide with their bid a copy of any and all Software Terms and Conditions or licenses that the State of West Virginia or the Agency will have to agree to or accept as a part of this solicitation. This information will be required before contract is issued.

5.3.3 Vendor should include a copy of any Maintenance Terms and Conditions or Licenses that the State of West Virginia or the Agency will be required to agree to and accept as a part of this solicitation. This information will be required before contract is issued.

5.3.4 Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

6 PERFORMANCE: Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already

included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

7 **PAYMENT:** Agency shall pay a flat fee, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

8 **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

9 **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

> **9.1** Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
>
> **9.2** Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
>
> **9.3** Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
>
> **9.4** Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
>
> **9.5** Vendor shall inform all staff of Agency's security protocol and procedures.

10 **VENDOR DEFAULT:** The following shall be considered a vendor default under this Contract.

10.1 Failure to perform Contract Services in accordance with the requirements contained herein.

10.2 Failure to comply with other specifications and requirements contained herein.

10.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.4 Failure to remedy deficient performance upon request.

10.5 The following remedies shall be available to Agency upon default:

10.5.1 Immediate cancellation of the Contract.

10.5.2 Immediate cancellation of one or more release orders issued under this Contract.

10.5.3 Any other remedies available in law or equity.

11 **MISCELLANEOUS:**

Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager:	aren ones, Dire tor o A inistration
Telephone Number:	804-750-5913
Fax Number:	
Email Address:	ones ls ata o

APPENDIX A:

SOFTWARE AS A SERVICE ADDENDUM

Begins on next page.

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:
  a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

5

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:
 a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
 b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
 c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
   - 10 days after the effective date of termination, if the termination is in accordance with the contract period
   - 30 days after the effective date of termination, if the termination is for convenience
   - 60 days after the effective date of termination, if the termination is for cause

  After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.
 d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
 e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

6

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:
   a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

7

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:
   a. Access and use the service for its business purposes;
   b. For SaaS, use underlying software as embodied or used in the service; and
   c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:_____   Name of Vendor:_____

Signature:_____   Signature:_____

Title:_____   Title:_____

Date:_____   Date:_____

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency:_____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐

2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐

3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐

5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: _____

   Email address: _____

   Phone Number: _____ _____

EXHIBIT A – Pricing Page
eDiscovery SaaS - (OT25112)

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.1	Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		$ -
4.12	Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		$ -
4.1.7	Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		$ -
4.1.7.4	Contract Item #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		$ -
4.1.7.5	Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		$ -
4.1.7.7	Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		$ -
4.1.8	Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		$ -
4.1.7.6	Contract Item #8: Maintenance and Support Year 1	LS	1.00		$ -
4.1.1	Optional Renewal Year 2: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		$ -
4.12	Optional Renewal Year 2: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		$ -
4.1.7	Optional Renewal Year 2:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		$ -
4.1.7.4	Optional Renewal Year 2: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		$ -
4.1.7.5	Optional Renewal Year 2: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		$ -
4.1.7.7	Optional Renewal Year 2: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		$ -
4.1.8	Optional Renewal Year 2: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		$ -
4.1.7.6	Optional Renewal Year 2: Contract Item #8: Maintenance and Support Year 1	LS	1.00		$ -
4.1.1	Optional Renewal Year 3: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		$ -
4.12	Optional Renewal Year 3: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		$ -
4.1.7	Optional Renewal Year 3:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		$ -
4.1.7.4	Optional Renewal Year 3: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		$ -
4.1.7.7	Optional Renewal Year 3: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		$ -
4.1.8	Optional Renewal Year 3: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		$ -
4.1.7.6	Optional Renewal Year 3: Contract Item #8: Maintenance and Support Year 1	LS	1.00		$ -
4.1.1	Optional Renewal Year 4: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		$ -
4.12	Optional Renewal Year 4: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		$ -
4.1.7	Optional Renewal Year 4:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		$ -
4.1.7.4	Optional Renewal Year 4: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		$ -
4.1.7.7	Optional Renewal Year 4: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		$ -
4.18	Optional Renewal Year 4: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		$ -
4.1.7.6	Optional Renewal Year 4: Contract Item #8: Maintenance and Support Year 1	LS	1.00		$ -
	Total Cost			$	-

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor Signature: _____   Date: _____

See Exhibit A Pricing Page Attached as a separate Excel attachment.

Please refer to Specification 5.3 for more information.

March 4th, 2025

Attn: BID CLERK
Department of Administration
Purchasing Division
2019 Washington St E
Charleston WV 25305

To whom it may concern,

LSP Data Solutions LLC, powered by Anvesa, provides eDiscovery and litigation technology services and software to both public and private sector clients of all scopes, industries, and sizes. We employ teams of experts with extensive relevant experience spanning a wide array of software platforms, data types and sizes, legal matters and investigations. Our services include data migration and management utilizing our cutting-edge SaaS solution, Anvesa, as well as end-to-end eDiscovery management, information governance consulting, legal hold, early case assessment (ECA), and forensic data collection.

Company Name	LSP Data Solutions LLC
Principle Address	1101 14th St NW, Suite 750
City, State Zip Code	Washington, D.C. 20005
UEID	JAQEKV58FTL3
CAGE Code	9HXC8
Website URL	https://lspdata.com
Principal Contact Name	Robert Chuey
E-Mail Address	rchuey@lspdata.com
Phone	202-924-1663

This submission is in response to the State of West Virginia's Centralized Request for Quote 0231 OOT2500000017 for Cybersecurity e-Discovery Software as a Service (OT25112). Thank you for your consideration and we hope to work with your team on this project.

Best Regards,

Robert Chuey
Cofounder and Managing Partner
LSP Data Solutions, LLC
202-924-1663

Company Overview

LSP Data Solutions LLC (LSP) was founded by industry leaders with over 60 years of combined experience providing eDiscovery and litigation technology services to law firms, corporations and government entities. We've leveraged this experience to solve the lack of transparency and excessive cost that has continued to plague the eDiscovery industry. Our unique approach revolutionizes the discovery process for our clients, allowing them to focus on the practice of law rather than technology concerns.

LSP partners with Anvesa to merge its industry-leading tools, functionality, and security with the unmatched service our company has become known for. Our expert teams of Litigation Support Professionals possess decades of experience in managing eDiscovery projects of all scopes and sizes, with clients including AM LAW 100 law firms, Fortune 500 companies, and government entities. LSP's Litigation Support Managers, eDiscovery Project Managers, Managed Review Attorneys, and Technical Data Analysts have managed and migrated hundreds of terabytes of data, comprising billions of documents and utilizing a wide range of eDiscovery and Forensic software platforms including Anvesa, QuikData, EDT, Relativity, EclipseSE, FTK, Cellebrite, Oxygen Forensics, and more.

By combining best-in-class technology with the expertise gained from handling thousands of complex matters, LSP prides itself in providing our clients with unparalleled service. We believe our extensive relevant experience makes our company precisely suited to the scope of this Request for Quote.

eDiscovery System Overview & Architecture

Overview

LSP utilizes Anvesa, a cloud-native, AI-powered **eDiscovery Software-as-a-Service (SaaS)** platform designed to handle the end-to-end electronic discovery process, from data ingestion and processing to document review, production, and reporting. Built on **Microsoft Azure**, Anvesa leverages a **scalable microservices architecture** with **Azure Kubernetes Service (AKS)** for dynamic resource allocation, ensuring high performance, reliability, and security.

Anvesa enables legal teams to efficiently manage large volumes of electronically stored information (ESI) with **self-service data loading, automated processing, advanced search and analytics, review, and production—all within a single platform**. The system eliminates the need for third-party integrations, offering a seamless and **fully automated workflow**.

Cloud-Native SaaS Architecture

Key Architectural Features:

- **Multi-Tenant & Scalable Infrastructure**: Supports multiple agencies and users with isolated, secure workspaces.

- **Azure Kubernetes Service (AKS)**: Auto-scaling compute and storage resources based on demand, ensuring seamless handling of high data volumes.

- **Microservices-Based Model**: Each core function (processing, search, review, production) runs independently, allowing for parallel execution without bottlenecks.

- **Serverless Auto-Scaling**: Eliminates the need for manual infrastructure management, ensuring cost efficiency and high availability.

- **Geo-Redundant Storage**: Ensures high availability and data resilience with replication across multiple Azure regions.

- **Role-Based Access Control (RBAC) & Single Sign-On (SSO)**: Provides granular permission settings and secure authentication.

- **Disaster Recovery & High Availability**: Automated failover mechanisms ensure continuous operations with minimal downtime.

Data Ingestion & Processing

- **Automated Bulk Ingestion**: Supports PST, ZIP, NSF, PDF, emails, chat data, and forensic images.

- **Metadata & Text Extraction**: Full-text indexing with **optical character recognition (OCR)** for scanned documents.

- **Embedded Object Processing**: Extracts attachments and inline images from emails and documents.

- **Data Culling & Filtering**: Supports **date range, custodian, keyword filtering, file type, and deduplication**.

- **DeNIST & Near-Duplicate Detection**: Identifies and removes redundant data to optimize review.

Advanced Review Capabilities

- **Unified Search & Filtering**: Boolean, fuzzy, proximity, wildcard, and AI-driven concept search.

- **Email Threading & Communication Graphs**: Organizes conversations for efficient contextual review.

- **Predictive Coding (TAR 2.0, TAR 3.0)**: AI-assisted document categorization and prioritization.

- **Interactive Review Dashboards**: Tracks case progress and reviewer performance in real time.

- **Multi-Format Viewer**: Supports native files, PDFs, multimedia, and structured data.

- **AI-Powered Redaction**: Automated **PII detection and redaction** for documents, images, and spreadsheets.

- **Multi-Language Translation**: In-platform language detection and translation.

Production & Export

- **Self-Service Production**: Users can generate productions in **Native, TIFF, PDF, and Load File formats**.

- **Automated QC & Validation**: AI-driven error detection before final export.

- **Metadata Handling & Bates Stamping**: Ensures compliance with legal requirements.

- **Load File Creation**: Compatible with **Relativity, Concordance, and other eDiscovery platforms**.

- **Secure Data Delivery**: Encryption-based export and **API integrations** for secure file transfers.

Security, Compliance & Disaster Recovery

- **Data Encryption**: AES-256 encryption for data **at rest and in transit**.

- **Multi-Factor Authentication (MFA) & Conditional Access**: Enforces secure login mechanisms.

- **Role-Based Access Control (RBAC)**: Ensures granular user permissions and access control.

- **SOC 2 Type II & ISO 27001 Certified**: Aligns with **FRCP, GDPR, HIPAA, and CCPA** security standards.

- **Audit Logs & Chain of Custody**: Ensures defensibility with a full history of user actions.

- **Automated Virus Scanning**: Detects malware and ensures file integrity before ingestion.

- **Disaster Recovery & High Availability**:
    - **Cloud-native auto-scaling** with **Azure Kubernetes Service (AKS)**.
    - **Geo-redundant storage** for data resilience.
    - **Automated backup, failover, and disaster recovery mechanisms**.

Performance & Scalability

- **Cloud-Native Deployment**: Built on Azure Kubernetes Service (AKS) for optimal performance.

- **Auto-Scaling Compute & Storage**: Dynamically allocates resources based on workload demand.

- **Microservices Architecture**: Modular, containerized services for improved fault tolerance and maintainability.

- **Handles Large Data Volumes**: Supports **multi-petabyte storage capacity**.

- **Processes Millions of Documents Simultaneously**: Ensures fast and efficient data handling.

- **Supports 50+ Concurrent Cases**: Without degradation in speed or performance.

- **Elastic Storage & Compute**: Scales automatically based on workload demands.

Conclusion

Anvesa's cloud-native, AI-driven eDiscovery platform provides a highly scalable, secure, and fully integrated solution for processing, reviewing, and producing ESI. With self-service capabilities, robust analytics, and AI-powered automation, Anvesa ensures faster insights, lower costs, and greater efficiency for legal teams handling complex litigation and regulatory investigations.

By leveraging modern cloud technologies, auto-scaling microservices, and enterprise-grade security, Anvesa delivers a future-ready eDiscovery solution that meets the demands of today's legal landscape.

System Administration & User Management

Anvesa's robust system administration and user management capabilities ensure scalability, security, and granular access control. With a cloud-native architecture built on Microsoft Azure, our platform enables efficient user provisioning, workspace management, and role-based access controls while maintaining enterprise-grade security.

User Management & Access Control

- **Unlimited User Seats** – Anvesa supports an **unlimited number of users** for at least 12 months, with licensing details covered in the **pricing section**.

- **Microsoft Office 365 Single Sign-On (SSO)** – Anvesa does not store user passwords; instead, authentication is seamlessly integrated with **Microsoft 365 SSO**, ensuring **password less authentication**.

- **Multi-Factor Authentication (MFA) & Conditional Access** – Supports **IP whitelisting** for office/home differentiation, enforcing MFA for external logins.

- **Role-Based Access Control (RBAC)** – Granular permissions management, ensuring that users only have access to what they need.

- **User Group-Based Access Control (UGBAC)** – Component-level security, allowing permissions to be defined at a **functional level** within the application.

- **Just-In-Time (JIT) Privileged Access** – Minimizing **standing administrative privileges** to reduce insider threats and unauthorized access.

- **User Role Toggle** – Administrators can **toggle between roles** to validate permissions, troubleshoot user access, and provide support.

- **Admin Controls for User & Data Management** – Client administrators have full control over **user creation, modifications, and removals**, ensuring secure access management.

Workspace & Configuration Management

- **Self-Service Workspace Creation** – Administrators can **independently create new workspaces**, configure security settings, and allocate storage based on case requirements.

- **Independent Case Management** – Each workspace is **isolated from others**, ensuring **secure and independent configurations per case**.

- **Customizable Permissions & Settings** – Admins can set up **custom user permissions, security policies, and data retention settings** at the workspace level.

- **Audit Logs & Activity Tracking** – Comprehensive **audit logs ensure full visibility** into user actions, permission changes, and system modifications.

Scalability & Performance

- **Scalable User Model** – Users can be **scaled up or down on a monthly basis**, based on the selected pricing model.

- **High-Performance Infrastructure** – Anvesa supports **any number of users**, leveraging a **scalable Azure-based environment** to dynamically allocate resources.

- **Cloud-Native Deployment** – Built on **Azure Kubernetes Service (AKS)** for optimized performance and auto-scaling.

Security & Compliance Enhancements

- **AES-256 Encryption at Rest & TLS Encryption in Transit** – Ensuring maximum data protection.

- **Microsoft Defender for Cloud & Azure Security Center** – Continuous **threat detection, monitoring, and automated remediation**.

- **Zero-Trust Security Model** – Enforcing **least privilege access** across all users, preventing unauthorized access to sensitive case data.

- **Two-Factor Authentication (2FA) & Single Sign-On (SSO)** – Ensuring **secure access through enterprise authentication methods**.

- **Automated Session Termination** – Users are **automatically logged out after inactivity**, preventing unauthorized access.

Conclusion

Anvesa's scalable and secure user management framework ensures efficient administration, robust security, and flexible licensing options. By leveraging Microsoft 365 SSO, RBAC, MFA, and audit logging, we provide seamless access control while maintaining enterprise-grade compliance.

Data Loading & Processing

Anvesa's cloud-native **Processing Tool** is designed to **handle high-volume electronic discovery** with **scalability, automation, and accuracy** at its core. Built on **Azure's scalable infrastructure**, Anvesa supports **self-service ingestion, metadata extraction, automated processing, and flexible export options** to meet the needs of legal teams handling complex cases.

Scalable & High-Performance Processing Engine

Anvesa's **processing engine** is built to handle **large-scale ingestion, processing, and filtering** while ensuring **maximum performance and efficiency**.

- **Azure-Powered Scalability:** Auto-scales compute and storage resources to accommodate increasing workloads.

- **Multi-Stage Processing:** Includes **Discovery, Processing, and Export** phases, ensuring a **structured and efficient workflow**.

- **Self-Service UI:** Users can **ingest, process, and load data into Anvesa** without backend intervention, making the system fully **self-service and user-friendly**.

- **Automated Error Handling & Reprocessing:** Identifies **corrupt, password-protected, or partially processed files** and reattempts processing automatically.

Bulk Data Ingestion & Multi-Layer Extraction

Anvesa supports **multiple file types and containerized data formats**, ensuring seamless ingestion from diverse sources:

- **Email Data:** PST, MBOX, NSF, MSG, EML.

- **Compressed Archives:** ZIP, 7z, RAR, TAR (including **nested containers** within PSTs, MSGs, or ZIP files).

- **Structured & Unstructured Data:** Office documents, PDFs, images, videos, chat data.

- **Cloud & Enterprise Sources:** OneDrive, SharePoint, Google Drive, AWS S3, Azure Blob.

Key Features:

- **Deep Extraction of Attachments & Inline Images:** Captures **all email attachments, embedded icons, and inline images** for complete email reconstruction.

- **Multi-Level Processing for Nested Containers:** Ensures extraction of **all files, even within deeply nested containers (e.g., PST inside PST, ZIP inside MSG).**

- **Self-Service Uploads & Web-Based Drag-and-Drop:** Users can **upload and process data directly from the UI**, eliminating the need for manual backend operations.

Automated Metadata Extraction & OCR Processing

Anvesa ensures all documents are **fully indexed and searchable** upon ingestion:

- **Comprehensive Metadata Capture:** Extracts file-level metadata (e.g., sender, recipient, timestamps, file size, hash values).

- **OCR for Scanned Documents & Handwritten Text:** Converts **image-based files, PDFs, and scanned documents** into searchable text.

- **Embedded Object & Hidden Metadata Extraction:** Detects **attachments, track changes, comments, and hidden elements** within documents.

Data Culling & Filtering

To **optimize review workflows**, Anvesa enables **advanced filtering and de-duplication** before document review:

- **Keyword & Boolean Filtering:** Enables **complex Boolean expressions, proximity search, and advanced keyword filtering.**

- **Global & Custodial Deduplication:** Eliminates redundant documents across **multiple custodians** and **data sets**.

- **DeNIST Processing:** Removes **non-relevant system files** (e.g., Windows executables, logs) to **reduce noise**.

- **Date Range & Metadata-Based Filtering:** Enables **targeted early case assessment (ECA)** by selecting relevant documents based on date, custodian, or metadata fields.

Self-Service Processing Templates

Anvesa allows users to **standardize and streamline processing workflows** using **custom templates**:

- **Pre-Configured & Custom Processing Profiles:** Automate **OCR, deduplication, metadata extraction, and indexing settings.**

- **Repeatable & Standardized Workflows:** Apply consistent **processing rules across multiple matters and custodians.**

- **Automated Load File Generation:** Exports **load files in DAT, CSV, and XML formats** compatible with **Relativity, Concordance, and Nuix.**

High-Speed Processing & Export Capabilities

Anvesa's processing engine is optimized for **speed and efficiency**, ensuring rapid turnaround for large-scale matters:

- **Parallel Processing Across Compute Nodes:** Distributes workloads across **Azure Kubernetes clusters** for high-throughput performance.

- **Processing Speed of Up to 1TB per Job:** Ensures **scalability for massive litigation matters** without performance degradation.

- **Multi-Format Export:** Supports **PDF, TIFF, Native, and Load File formats** for seamless production.

- **Automated Production Readiness:** Ensures **all metadata, redactions, and privilege logs** are accurately captured before export.

Why Anvesa for Data Loading & Processing?

- ✓ **End-to-End Self-Service:** Users can **ingest, process, filter, and load data** with minimal intervention.
- ✓ **AI-Driven Automation:** Advanced **deduplication, metadata extraction, and culling** reduce review workloads.
- ✓ **Cloud-Native Scalability: Auto-scales compute and storage** to handle **1M+ documents per case.**
- ✓ **Optimized for Large-Scale Matters:** Handles **complex nested containers**, **multi-format exports**, and **automated error handling**.
- ✓ **Secure & Compliant:** Adheres to **FRCP, GDPR, CCPA**, ensuring **full audit trails and defensibility**.

Anvesa's **powerful data ingestion and processing engine** provides **high-speed, automated, and scalable** solutions for legal teams handling **large volumes of ESI**, ensuring **faster insights, reduced costs, and efficient eDiscovery workflows.**

Document Review & Advanced Analytics

Fast & Scalable Review Environment

Anvesa's cloud-native eDiscovery platform is designed for high-performance document review, supporting **concurrent cases**, each with over **1 million documents**, without performance degradation. Leveraging **Azure Kubernetes Service (AKS)** and an **auto-scaling infrastructure**, Anvesa dynamically adjusts compute resources to ensure a seamless review experience, even under heavy workloads.

Key features of Anvesa's review environment include:

- **High-Speed Document Rendering:** Instant document loading and rendering across multiple file types.

- **Batch Review Management:** Efficient document allocation to reviewers with real-time progress tracking.

- **Customizable Review Workspaces:** Users can organize and manage documents with flexible foldering and tagging options.

- **Secure, Multi-Tenant Access:** Role-based access control (RBAC) ensures ethical walls and permissions for different teams.

Advanced Search & Analytics

Anvesa provides powerful search capabilities that go beyond basic keyword searches, ensuring users can locate relevant documents with precision.

Advanced Search Features:

- **Boolean Search** – Supports AND, OR, NOT operators for precise query construction.

- **Proximity & Fuzzy Search** – Finds terms within a specific range and accommodates variations in spelling.

- **Stemming & Wildcard Searches** – Extends searches to variations of root words and unknown characters.

- **Concept Search** – AI-driven contextual search that retrieves conceptually relevant documents.

Email Threading & Communication Graphs

- **Threaded Email Review** – Automatically groups related emails to maintain contextual integrity.

- **Communication Graphs** – Visualizes communication patterns across custodians, helping identify key players in litigation.

AI-Assisted Review & Predictive Analytics

Anvesa integrates advanced AI and **Technology-Assisted Review (TAR)** methodologies to optimize the document review process:

- **Predictive Coding (TAR 2.0, TAR 3.0)** – AI models prioritize relevant documents, reducing manual review time.

- **Topic & Document Clustering** – AI-powered thematic grouping for enhanced review efficiency.

- **Near-Duplicate Detection** – Identifies and groups similar documents to minimize redundant review efforts.

- **Active Learning** – Continuously refines AI models based on reviewer decisions, improving classification accuracy.

Visual Analytics: Word Clouds & Email Subject Cloud

Anvesa provides **visual insights** into document sets through **dynamic data visualization tools**, making it easier to uncover trends and key themes.

- **Word Cloud:** Generates a real-time visual representation of the most frequently occurring words within the dataset.

- **Email Subject Cloud:** Extracts and displays **key terms from email subjects**, enabling quick identification of important topics.

These features **enhance early case assessment (ECA)** by surfacing **critical case trends** at a glance, allowing users to **prioritize high-value documents.**

PII Detection & Redaction

Anvesa ensures data privacy and compliance with built-in **PII detection and automated redaction** features.

- **Multi-Format Redaction:** Supports redacting **documents, images, and Excel spreadsheets**.

- **Customizable Redaction Workflows:** Users can create and apply redaction templates for consistency.

- **Audit Logging:** Full transparency and tracking of redaction actions for defensibility.

Video & Audio Analysis

Anvesa extends AI-powered analytics to multimedia content, enabling faster review of **video and audio evidence.**

- **Speech-to-Text Transcription:** Converts spoken words into searchable text.

- **Scene Detection & Emotion Analysis:** Identifies key moments, speakers, and sentiment in videos.

- **Keyword & Concept Extraction:** AI highlights important topics for faster review.

Upcoming Generative AI Innovations in Anvesa

Anvesa is continuously evolving, and our **next-generation AI capabilities** will redefine how legal teams interact with data:

1. Generative AI-Based Search (Conversational Search)

- **LLM-Powered Chat Interface:** Users can interact with documents using **natural language queries** instead of traditional keyword searches.

- **Contextual Understanding:** AI understands **case-specific context**, delivering **more precise search results.**

2. Enhanced Predictive Coding with LLMs

- **Self-Learning AI Models:** Continuously improve classification accuracy by learning from reviewer decisions.

- **Intelligent Prioritization:** Automatically ranks **high-relevance documents**, reducing time spent on non-essential reviews.

Shaping the Future of eDiscovery with Anvesa

Anvesa combines **high-speed document review, advanced AI analytics, and scalable infrastructure** to deliver an industry-leading eDiscovery experience. By automating **document classification, search, and redaction**, legal teams can **reduce costs, accelerate case timelines, and maintain compliance** with evolving regulations.

With **AI at its core,** Anvesa **enhances accuracy, reduces costs, and ensures compliance** at every stage. Our commitment to innovation ensures your legal team stays **ahead of the curve.**

Production Module

Anvesa's Production Module is a self-service, scalable, and highly configurable solution designed for effortless, defensible, and efficient document production. It offers seamless export options, automated quality control, and compliance-driven workflows, ensuring that legal teams can quickly generate and deliver productions with full auditability and security.

Self-Service Production & Multi-Format Export

Anvesa provides a **completely self-service production workflow**, allowing users to configure, validate, and finalize productions independently. The system supports:

- **Multi-Format Production Outputs:**

    - **TIFF Productions:** Single-page and multi-page TIFF exports.

    - **PDF Exports:** Single-page **searchable PDFs**, **multi-page searchable PDFs**, and **multi-page non-searchable PDFs**.

    - **Native File Productions:** Exports documents in their **original format** to maintain authenticity.

    - **Text & Load File Exports:** Supports **DAT, OPT,LFP ,CSV and LST load files** with **metadata fields, extracted text, and document tags** for seamless integration with review platforms like **Relativity, Nuix, and Concordance**.

- **Customizable Production Settings:**

    - Supports **page-level previews** before finalizing exports, ensuring accurate **endorsement, Bates numbering, and redaction verification**.

    - Configurable **single-page vs. multi-page exports** based on **project requirements**.

- **Automated Load File Generation:**

    - Ensures **industry-standard metadata formats** to maintain compatibility with external review platforms.

- **Scalable Production Infrastructure:**

    - Automatically **scales computing power** based on the **size and complexity** of the production set, ensuring rapid execution.

    - Allows users to **run multiple productions in parallel** without system degradation.

- **Secure Production Download & Delivery:**

    - Completed productions are delivered via high-security download links, protected by SAS tokens with expiration controls for restricted access, which reduces the copy and upload time when sharing with the client.

Automated Bates Stamping, Endorsements, & Redaction Management

Anvesa provides **fully automated** Bates stamping, endorsements, and redaction tools to ensure **consistent document handling** across all productions.

- **Bates Numbering & Custom Endorsements:**

    o Configurable **prefixes, suffixes, numbering sequences, and positioning options**.

    o Supports **confidentiality labels, custom text stamps, and field-based endorsements**.

- **Mass Redaction & Annotation Management:**

    o **Automated redactions** for **PII, privileged content, and sensitive information**.

    o Supports **metadata redaction** and **burn-in redactions** for all exported formats.

- **Endorsement & Page-Level Preview:**

    o Users can **preview endorsements, Bates stamps, and redactions** before executing production.

Wizard-Driven Production Workflow & Pre-Production Validation

Anvesa simplifies **complex production workflows** with an intuitive **wizard-driven interface**, guiding users through:

1. **Document Selection & Redaction Review:** Ensures **all confidential content is protected** before finalizing export.

2. **Bates Numbering & Endorsements:** Allows **custom configurations** for numbering schemes, branding, and legal markings.

3. **Production Format & Load File Selection:** Users can choose **TIFF, PDF, Native, and Load File formats** with customizable metadata fields.

4. **Production Summary & Pre-Validation:**

    o **Comprehensive production summary** displays **document counts, redaction checks, and metadata validations** before execution.

    o Detects **missing fields, duplicate Bates numbers, and incomplete redactions**, preventing **errors before production is finalized**.

Privilege Log Creation & Legal Compliance

Anvesa ensures privileged content is **properly tracked, logged, and protected**, maintaining full **compliance with legal and regulatory requirements**.

- **Automated Privilege Log Generation:**

    o Tracks **withheld or redacted documents**, ensuring legal teams **can justify exclusions.**

    o Generates **detailed logs** with customizable privilege codes, reason fields, and attorney-client designation labels.

- **Audit Trail & Compliance Reports:**

    o Comprehensive tracking of **every user action**, including **redaction edits, privilege designations, and final export logs**.

    o **Compliance with FRCP, GDPR, CCPA, FOIA, and HIPAA** ensures defensibility in legal proceedings.

Why Choose Anvesa's Production Module?

- ✓ **Self-Service & Fully Automated:** Users can **independently configure, validate, and export productions** without IT intervention.
- ✓ **Flexible Export Options:** Supports **TIFF, PDF, Native, and Load File formats** for **industry-standard compatibility**.
- ✓ **Defensible Bates Stamping & Redaction Workflows:** Ensures **accurate, consistent, and legally defensible document handling**.
- ✓ **Wizard-Driven, Error-Free Process: Pre-validation & production summaries** eliminate **costly errors** before execution.
- ✓ **Secure & Scalable Production:** Auto-scales processing power and delivers productions **via highly secure, SAS-protected download links**.

Anvesa's Production Module provides unparalleled efficiency, compliance, and security, ensuring legal teams can generate and deliver productions with confidence, speed, and precision.

Reporting and Analytics

Anvesa empowers legal teams with real-time, actionable insights across data processing and review. Our platform provides granular, data-driven reports tailored to the needs of law firms, document review companies, corporations, and government agencies—ensuring transparency, efficiency, and defensibility throughout the e-discovery lifecycle.

Regular Status Reports on Data Processing and Review Progress:

Anvesa Processing Tool Reports:

- Our processing tool generates detailed insights at every stage—Discovery, Processing, and Export—ensuring complete visibility into the data lifecycle.

- Discovery Phase Reports include:
    - Deduplication statistics: Breakdown of unique and duplicate documents.
    - File type classification: Extension-wise breakdown for document categorization.
    - Processing progress: Live tracking of processing completion percentage and document counts.

- Custodian and Job-Level Reporting:
    - For each custodian and job, Anvesa provides a comprehensive summary of:
        - Number of discovered, processed, and exported documents.
        - Total number of exports conducted.
    - Reports can also be generated at the matter level for consolidated insights across multiple jobs.

Review Progress Reports:

- **Batch Review Status Reports:**
    - Tracks assigned and unassigned documents, as well as their review status (e.g., in review, on hold, unreviewed).

- **Usage Reports:**
    - Provides user-based metrics over a selected date range, including:
        - Total and exact review usage time.
        - Total views, unique views, and average views per hour.
        - Total page views, bulk edits, and unique edits per hour.

- **Additional Review Reports:**
    - Privilege Report
    - Document Audit Report

- o PII Report

- o Overturn Report

- o Unviewed Document Report

- o Video Faces Report

- o Each report is designed for granular analysis, ensuring in-depth tracking and compliance oversight.

Analytics on Data Volumes, Review Speeds, and Key Metrics:

Anvesa provides real-time analytics on:

- **Data Volumes:**
  - o Tracks total documents ingested, processed, and reviewed per job, custodian, or across matters.

- **Review Speeds:**
  - o Measures reviewer performance, including average documents reviewed per hour and batch completion times.

- **Key Metrics:**
  - o Provides insights into reviewer decisions, overturn trends, PII detection rates, and more.

Customizable Dashboards for Real-Time Project Monitoring:

- **Dynamic Review Dashboards:**
  - o Our interactive dashboards track document review progress, customizable with facetable fields for tailored insights.

- **Drill-Down Analytics:**
  - o Users can click on any parameter to further refine and analyze specific aspects of the dataset.

- **Search Synchronization:**
  - o Maintains search consistency across modules, allowing users to apply saved searches seamlessly throughout workflows.

- **Timeline Tracking:**
  - o Enables teams to log and track key events, ensuring smooth project management and review execution.

Conclusion: Why Anvesa?

- **End-to-End Transparency:** Our platform ensures full visibility into processing and review, enabling informed decision-making.

- **Efficiency-Driven Analytics:** Optimized performance tracking to enhance workflows and eliminate bottlenecks.

- **Customizable and Scalable:** Tailored dashboards and reports designed to fit diverse client needs.

- **Industry Compliance:** Supports best practices in line with FRCP, GDPR, and CCPA standards.

By leveraging Anvesa's robust reporting and analytics framework, clients can maximize operational efficiency, ensure defensibility, and drive informed legal strategy with confidence.

Security & Compliance

Security is embedded at every layer of Anvesa's **cloud-native e-discovery platform** and serves as a foundational pillar of our solution. Fully deployed on **Microsoft Azure**, we leverage its comprehensive security features while adhering to stringent regulatory and industry standards. Our **zero-trust security model** ensures **data confidentiality, integrity, and availability** throughout the **e-discovery lifecycle**. With robust encryption protocols, strict access controls, and continuous compliance monitoring, we proactively safeguard client data, ensuring adherence to industry regulations and corporate security mandates.

Current Security Measures

1. **Security Protocols and Certifications**
   Anvesa benefits from Microsoft Azure's highly secure cloud infrastructure, inheriting its extensive security compliance and certifications, including:

   - ✓ **ISO/IEC 27001** – International standard for Information Security Management Systems (ISMS).
   - ✓ **SOC 1, SOC 2, and SOC 3** – Compliance for service organizations with critical security controls.
   - ✓ **FedRAMP Moderate** – Ensuring compliance for handling federal data where applicable.
   - ✓ **GDPR and HIPAA Compliance** – Adhering to global data privacy and protection regulations.
   - ✓ **Microsoft Defender for Cloud** – Continuous threat detection and automated remediation.
   - ✓ **Azure Security Center** – Proactive security posture management across all Azure services.

   Additionally, Anvesa implements strict user access management controls, including:

   - ✓ **Multi-Factor Authentication (MFA) with Conditional Access** – Supports IP whitelisting for seamless login from office locations while enforcing MFA for external access.
   - ✓ **Microsoft-backed Single Sign-On (SSO)** – All authentication and password management are fully controlled by the customer's Microsoft account, ensuring enterprise-grade security.
   - ✓ **Azure Role-Based Access Control (RBAC)** – Granular access management across all Azure resources and services, ensuring users only access what they need.
   - ✓ Encryption at rest and in transit using **AES-256** and **TLS** protocols to ensure the highest level of data security

2. **Penetration Testing & Vulnerability Assessments**

   Anvesa has undergone rigorous penetration testing and vulnerability assessments conducted by an ISO-certified third-party security firm, ensuring the highest level of security. Testing methodology follows:

   - ✓ **OWASP Top 10** – Protection against critical web application security risks.
   - ✓ **SANS Top 25** – Identification and mitigation of dangerous software vulnerabilities.
   - ✓ **API Security Testing** – Endpoint integrity protection against unauthorized access.
   - ✓ **Zero-Day Threat Simulation** – Testing resilience against unknown vulnerabilities.
   - ✓ **Logical Checks & Application-Specific Validations** – Custom security assessments for platform robustness.

   As a result, Anvesa has successfully obtained a **"Safe to Host"** certification, confirming our adherence to industry best practices and secure deployment readiness.

3. **Disaster Recovery & Business Continuity**

   Ensuring business continuity is critical in litigation support. Anvesa has a resilient disaster recovery (DR) strategy that provides:

   - ✓ **Cloud-native auto-scaling** with **Azure Kubernetes Service (AKS)**.

   - ✓ **Geo-redundant storage** for data resilience and multi-region failover.

   - ✓ **Automated backup and failover mechanisms** ensuring near-zero downtime.

   - ✓ **Regular disaster recovery (DR) testing** – Validating **Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)** to meet SLA commitments.

   - ✓ **Immutable backup policies and versioning** – Ensuring data integrity for litigation and compliance purposes.

4. **Cloud-Native Security Advantages**

   Anvesa is a fully cloud-native application, eliminating the need for traditional virtual machines, which often introduce security risks related to patching, OS management, and misconfigurations. This approach provides:

   - ✓ Seamless auto-scaling and auto-patching with no server maintenance overhead.
   - ✓ Security recommendations and real-time monitoring from Azure Security Center.
   - ✓ Automatic updates and compliance enhancements, ensuring continuous alignment with evolving regulations.

By default, Anvesa services are monitored, patched, and secured via Azure's infrastructure, ensuring a highly secure, reliable, and scalable environment without requiring traditional server or virtual machine management.

Future Security Roadmap

Anvesa continuously strengthens its security framework to stay ahead of emerging threats and compliance requirements. Over the next 12-24 months, it is focused on implementing the following enhancements:

1. **AI-Powered Threat Detection & Automated Response**
   - Introducing AI-driven behavioral analytics to detect anomalies and potential insider threats.
   - Implementing automated response workflows for faster containment of security incidents.
2. **Zero-Trust Expansion & Continuous Authentication**
   - Just-In-Time (JIT) access for critical operations, reducing standing administrative privileges.
   - Continuous authentication mechanisms, such as behavioral biometrics, to prevent credential-based attacks.
3. **Automated Compliance & Governance Enhancements**
   - Strengthening AI-driven compliance automation to proactively detect and address regulatory changes.
   - Expanding governance policies beyond existing compliance frameworks (GDPR, HIPAA) to address new industry-specific mandates.
4. **Client-Controlled Encryption & Data Sovereignty**
   - Implementing Client-Managed Encryption Keys (CMEK) to give enterprises more control over encryption and data sovereignty.
   - Enhancing data residency controls to align with evolving global privacy laws.
5. **Ongoing Penetration Testing & Security Hardening**
   - Regular penetration testing of the Anvesa platform to identify and mitigate security vulnerabilities proactively.
   - Conducting third-party security assessments to validate Anvesa's resilience against evolving cyber threats.
6. **Continuous Security Releases & Azure Security Best Practices**
   - Implementing Microsoft Azure Security Recommendations across all services to improve Anvesa's security posture.
   - Continuously applying Azure-backed security patches and updates to maintain a high Secure Score and adhere to Microsoft's best practices.

Commitment to Security & Compliance Excellence

Anvesa is committed to **proactive security, regulatory compliance, and continuous innovation**. Our **security-first approach** ensures that law firms, corporations, and government agencies can **trust our platform** to handle sensitive data with the highest level of protection. We remain committed to proactively evolving our security framework to counter emerging cyber threats, adapt to evolving regulations, and uphold the highest standards of data protection—solidifying Anvesa as a trusted partner in legal technology.

Migration and Implementation Services

LSP Data has guided numerous organizations through the migration of active data projects employed on a range of eDiscovery platforms. LSP's broad experience in this area has earned us a reputation as experts in data migration, even being sought out to perform as technical support subcontractor for other eDiscovery software companies to assist their clients with their own migrations between systems. A successful migration between software platforms requires enormous attention to detail, and a dedication to a real-time problem-solving mentality. The most critical role is to quickly identify problems that are not readily transparent within the originating or target software environments.

Use Case

One example of LSP successfully performing complex data migration was as the Prime Contractor for a large national litigation matter involving dozens of pharmaceutical manufacturers, distributors, and national pharmacy retailers. The case involved over 15 terabytes of data, including emails, chat messages, financial records, transactional database data, marketing materials, and other data formats. LSP was responsible for managing the entire project including data collection and migration, processing, managed review, data analysis, production, and quality control.

The data for this matter was migrated between two enterprise eDiscovery management and review software platforms during active litigation, requiring a tiered and well-documented process to ensure no deadlines were missed, and access to data during discovery was unaffected. LSP collaborated with the legal team to create a priority-driven plan to implement this data into the new system. The original system was kept online while the new platform was built and a rolling data ingestion populated. The plan included action and quality control items for various tasks, including: database creation, field set up, user account creation, tagging and coding setup and matching, data analysis from original database, export and backup processing, quality control of export package, import compatibility, field matching upon import, document matching upon import, text matching upon import, image matching upon import, extracted and OCR text indexing, viewer confirmation, coding and tagging field confirmation of imported data, search accuracy confirmation, and other items. Every step required confirmation by technical and project management team members to ensure client personnel were provided a seamless experience post-migration. With concurrent activity occurring while the migration was in progress, there were additional tasks necessary to ensure work product which was migrated as a final step. Much of this was performed outside normal business hours to ensure minimal downtime was experienced by the users, allowing them to access the new database the next business day with zero interruption to their workflow.

The first step in the migration process was to collect and ingest the data from various client systems. This involved identifying all relevant data sources and using specialized software tools to extract and process the data. Tools used by LSP to collect data include Cellebrite UFED, FTK Imager, Magnet Axiom, Pinpoint Harvester, Tableau TD3 Imaging Hardware, BlackBagTechnologies Mac Collector, Microsoft 365 eDiscovery, and Rocket Remote Collector. The data was then processed and loaded into the document hosting platform for review by the team of attorneys and paralegals. The project also included hundreds of data sources of incoming document productions

from opposing firms. These incoming production volumes required extensive modifications to ensure they were complete and without error prior to loading into the document review platform. LSP staff identified errors with hundreds of production deliverables received from other service providers, and litigation support departments including: skipped bates numbers, missing or incorrect metadata fields, inaccurate delimiters for the load files, missing images, text and native files, corrupt files, and other issues. LSP's eDiscovery Technology Team reported the identified errors to counsel, and recommended steps for remediations.

Methodology

LSP has migrated numerous projects that were in active litigation, requiring a tiered and well-documented process to ensure timely responses to all deadlines, and access to data was unaffected. The process of migrating cases during open litigation requires communication, coordination, and documentation to safeguard a successful and painless experience.

LSP will work with the attorneys and staff to a create priority driven plan to transition the data into the new system in a logical, efficient and methodical manner. Through the migration process the original system can be kept online and active. LSP would take all necessary steps to fast-track the migration process, being mindful of the financial impact on the client. Accomplishing this requires a coordinated effort of the extensive experience of the LSP team along with the client. An implementation plan would include the following action items:

- Database creation and quality control to ensure settings (de-duplication, time zone, etc.) are accurate.
- Field set up and quality control for naming, field type, security, etc.
- User access creation and permission controls.
- Tagging and coding setup, matching field type, security, etc.
- Coding panel creation, security, etc.
- Data analysis from original database (document counts, work product, folder formats, saved searches, etc.)
- Export and backup processing.
- Quality control of export package.
- Import compatibility analysis.
- Field matching upon import and confirmation.
- Document matching upon import.
- Text matching upon import.
- Image matching upon import.
- Extracted and OCR text indexing.
- Viewer confirmation (check random sampling and varied file types to ensure viewers accurately display documents.)
- Coding and tagging field confirmation of imported data.
- Search accuracy confirmation.
- Redaction confirmation and accuracy.
- Other items as necessary dependent on case and data specific needs.

Every step in the migration process requires coordination by the technical and project management team members to ensure a seamless experience post-migration. With the sensitive nature of eDiscovery data and privileged information, it is imperative that security permissions and work products are not compromised. Once the source database is no longer needed, LSP manages the appropriate destruction of data in all its forms (text, native files, images, database records, etc.) is purged using industry standards, with no capacity for retrieval.

With concurrent activity occurring during the migration process, there are necessary additional steps that must be implemented to capture additional work product that was created. The work product created must be accounted for and accurately migrated to the target project in the new platform's instance. Best practice is to perform the final steps outside normal business hours guaranteeing minimal downtime with zero interruption to users' workflow.

Training and Support

LSP's team of Project Managers and eDiscovery Consultants have decades of experience assisting clients with every phase of the EDRM and discovery process. Our dedicated staff of experts can assist on matters related to:

- Legal hold and data retention
- Custodian interviews
- Digital Forensics and data collection
- Data investigations
- Data processing and ingestion
- Third party custom data collection and integration for review
- ESI Protocol creation and editing
- Document review protocols and workflows
- eDiscovery database set up and organization
- Document production creation and customization
- AI and Analytics technology adoption and use

LSP provides around the clock Project Management support for legal teams and **unlimited administrative and end-user training** to cover the entire functionality of our eDiscovery solution, Anvesa, depending on the specific needs of the users.

Training would primarily take place virtually and would be offered at any time a user needed to learn additional functions of the solution. In-person training sessions can also be scheduled as needed, in both group and one-on-one formats. Training subject matter would be tailored to the needs of the user(s) taking part in the session.

LSP recommends numerous training sessions for users to develop familiarity with Anvesa's software platform. Training sessions can be scheduled at varied times of day to accommodate users' schedules. Additional one-on-one training sessions can be provided upon user request.

LSP's team of experts will be available to support legal teams as needed to ensure full access and successful implementation, including:

- Collaborating with the legal team on the data parameters for existing case data to be migrated.

- Communicating with the legal team on case specifications and database setup parameters required to ensure a seamless transition.

- Communicate with staff regarding timelines to ensure project deadlines are met.

- Consult on and provide cost-saving archived storage for idle projects as needed.

- Identify follow-up opportunities for additional knowledge base sessions.

References

Robert A. Eisenberg, Esq., CMLaw/EPC
eDiscovery Counsel
Marc J Bern & Partners LLP
One Grand Central Place
60 East 42nd Street, Suite 950
New York, New York 10165
212.702.5000 Ext. 563
reisenberg@BernLLP.com

Charlie Black, owner
Pro Legal Tech
907 S. Detroit Ave
Suite 1004
Tulsa, OK 74120
918.584.2525
Charlie@prolegaltech.com

Quentin Templeton, Partner
Fagan & Emert
800 New Hampshire St.
Suite 110
Lawrence, KS 66044
785.331.0300
qtempleton@faganemert.com

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.1	**Contract Item #1:** Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	$ -	$ INCLUDED
4.12	**Contract Item #2:** One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	$ 3.00	$ 250.00
4.1.7	**Contract Item #3:** Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	$ -	$ INCLUDED
4.1.7.4	**Contract Item #4:** e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	$ -	$ INCLUDED
4.1.7.5	**Contract Item #5:** Initial Setup and configuration of eDiscovery SaaS	LS	1.00	$ -	$ INCLUDED
4.1.7.7	**Contract Item #6:** e-Discovery SaaS Project Management	HR	100.00	$ 150.00	$ 15,000.00
4.1.8	**Contract Item #7:** e-Discovery SaaS Technical Support	HR	100.00	$ -	$ INCLUDED
4.1.7.6	**Contract Item #8:** Maintenance and Support Year 1	LS	1.00	$ -	$ INCLUDED
4.1.1	**Optional Renewal Year 2: Contract Item #1:** Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	$ -	$ INCLUDED
4.12	**Optional Renewal Year 2: Contract Item #2:** One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	$ 3.50	$ 300.00
4.1.7	**Optional Renewal Year 2:Contract Item #3**: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	$ -	$ INCLUDED
4.1.7.4	**Optional Renewal Year 2: #4:** e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	$ -	$ INCLUDED
4.1.7.5	**Optional Renewal Year 2: Contract Item #5:** Initial Setup and configuration of eDiscovery SaaS	LS	1.00	$ -	$ INCLUDED
4.1.7.7	**Optional Renewal Year 2: Contract Item #6:** e-Discovery SaaS Project Management	HR	100.00	$ 160.00	$ 16,000.00
4.1.8	**Optional Renewal Year 2: Contract Item #7:** e-Discovery SaaS Technical Support	HR	100.00		$ INCLUDED
4.1.7.6	**Optional Renewal Year 2: Contract Item #8:** Maintenance and Support Year 1	LS	1.00	$ -	$ INCLUDED
4.1.1	**Optional Renewal Year 3: Contract Item #1:** Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	$ -	$ INCLUDED
4.12	**Optional Renewal Year 3: Contract Item #2:** One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	$ 4.00	$ 350.00
4.1.7	**Optional Renewal Year 3:Contract Item #3**: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	$ -	$ INCLUDED
4.1.7.4	**Optional Renewal Year 3: #4:** e-Discovery SaaS access to an online knowledge base or help center.	LS INCLUDED	1.00	$ -	$ INCLUDED
4.1.7.5	**Optional Renewal Year 3: Contract Item #5:** Initial Setup and configuration of eDiscovery SaaS	LS	1.00	$ -	$ INCLUDED
4.1.7.7	**Optional Renewal Year 3: Contract Item #6:** e-Discovery SaaS Project Management	HR	100.00	$ 170.00	$ 17,000.00
4.1.8	**Optional Renewal Year 3: Contract Item #7:** e-Discovery SaaS Technical Support	HR	100.00		$ INCLUDED
4.1.7.6	**Optional Renewal Year 3: Contract Item #8:** Maintenance and Support Year 1	LS	1.00	$ -	$ INCLUDED
4.1.1	**Optional Renewal Year 4: Contract Item #1:** Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	$ -	$ INCLUDED
4.12	**Optional Renewal Year 4: Contract Item #2:** One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	$ 4.50	$ 400.00
4.1.7	**Optional Renewal Year 4:Contract Item #3**: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	$ -	$ INCLUDED
4.1.7.4	**Optional Renewal Year 4: #4:** e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	$ -	$ INCLUDED
4.1.7.5	**Optional Renewal Year 3: Contract Item #5:** Initial Setup and configuration of eDiscovery SaaS	LS	1.00	$ -	$ INCLUDED
4.1.7.7	**Optional Renewal Year 4: Contract Item #6:** e-Discovery SaaS Project Management	HR	100.00	$ 180.00	$ 18,000.00
4.18	**Optional Renewal Year 4: Contract Item #7:** e-Discovery SaaS Technical Support	HR	100.00		$ INCLUDED
4.1.7.6	**Optional Renewal Year 4: Contract Item #8:** Maintenance and Support Year 1	LS	1.00	$ -	$ INCLUDED
	Total Cost			$	67,300.00

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Robert Chesey
Vendor Signature: **Date:** 03/04/2025