The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

wvOASIS

Welcome, Robert M Ross

Solicitation Response(SR) Dept: 0803 ID: ESR06282300000006647 Ver.: 1 Function: New Phase: Final ▼ Modified by batch , 06/28/2023

Header 🔗 10

List View

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

Procurement Folder: 1234689

Procurement Type: Central Master Agreement

Vendor ID: VS0000041967

Legal Name: AUDITBOARD INC

Alias/DBA:

Total Bid: $0.00

Response Date: 06/28/2023

Response Time: 11:43

Responded By User ID: smergenthal01

First Name: Sean

Last Name: Mergenthal

Email: smergenthal@auditboard.com

Phone: 8563817892

SO Doc Code: CRFQ

SO Dept: 0803

SO Doc ID: DOT2300000145

Published Date: 6/16/23

Close Date: 6/28/23

Close Time: 13:30

Status: Closed

Solicitation Description: Auditing SaaS RFQ (81230134)

Total of Header Attachments: 10

Total of All Attachments: 10

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:	1234689
Solicitation Description:	Auditing SaaS RFQ (81230134)
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2023-06-28 13:30	SR 0803 ESR06282300000006647	1

VENDOR
VS0000041967 AUDITBOARD INC

Solicitation Number:	CRFQ 0803 DOT2300000145				
Total Bid:	0	**Response Date:**	2023-06-28	**Response Time:**	11:43:36

Comments: Please see all attachments for technical response and commercial terms. We do not offer discounts for early payment. However, if AuditBoard is awarded the contract, we can discuss volume discounts or multi-year commitment discounts depending on timing, number of licenses purchased, etc.
We understand that per your general terms and conditions, by submitting documentation through wvOasis we have reviewed this Solicitation/Contract in its entirety and will comply with the requirements unless otherwise stated (such as termination for convenience clause).

FOR INFORMATION CONTACT THE BUYER
Larry D McDonnell
304-558-2063
larry.d.mcdonnell@wv.gov

Vendor
Signature X   **FEIN#**   **DATE**
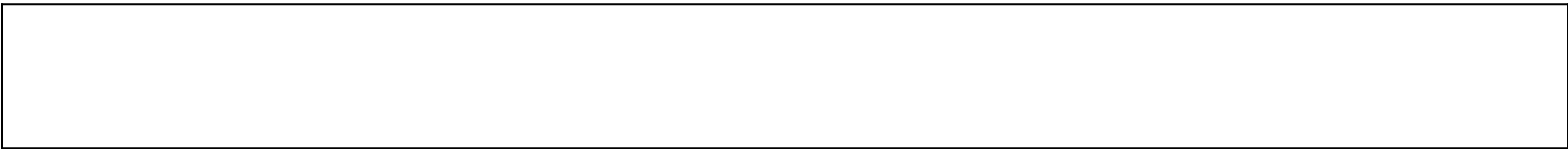
All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Cloud-based software as a service	0.00000	EA	990750.000000	0.00

Comm Code	Manufacturer	Specification	Model #
81162000			

Commodity Line Comments: See attachments for commercials. Total unit price above is inclusive of all optional items. Delivery is approximate based on 10 week implementation. We thank the state of West Virginia and Department of Transportation for the opportunity to bid on the Auditing SaaS RFQ and we are excited about the partnership. While we meet all the technical requirements you have listed in the RFQ and specifications document, we believe that any partnership that can be terminated unilaterally without cause is not a true partnership. As such, we take exception to termination for convenience language that you have included in documents related to the RFQ. We are happy to review terms and conditions with you and even utilize your terms and template as the starting point for contract negotiations, however we will not enter into an agreement that contains a termination for convenience clause. Our standard agreements contain protection for you as the customer, including termination of contract for cause or breech of contract, but simply for convenience is not a true partnership and we are committed the partnership. As such, we have submitted the documents and ask that you please reconsider. Our legal team will not entertain this one point but is open to negotiating otherwise. AuditBoard is the top rated audit solution on the market and we believe we are the best fit for Dawna Cork and the WVDOT team when we have spoken with them. Thank you again for the opportunity to do business with WVDOT.

Extended Description:

Auditing SaaS RFQ (81230134). See attached pricing page and CRFQ documentation.

AUDITBOARD

RFQ Response for Auditing Cloud-Hosted SaaS (Cost Proposal)

SOLICITATION NO.:   CRFQ 0803 DOT2300000145

PRESENTED TO

Larry McDonnell, Senior Buyer

*Per Section 21 of your instruction to vendors, if awarded and you are going to publish our proposal to a public website, we are more than happy to provide a redacted version.

SALES ADVISORY TEAM

Sean Mergenthal, Account Executive
Mike Rissmiller, Manager Product Solutions

June 28, 2023

AUDITBOARD

AuditBoard, Inc.
12900 Park Plaza Drive, Suite 200
Cerritos, CA 90703

June 28, 2023

West Virginia Department of Transportation
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Attn: Larry McDonnell

RE: AuditBoard RFQ response to WVDOT

Dear Mr. McDonnell,

On behalf of AuditBoard, Inc. ("AuditBoard" or "We"), we thank you for the opportunity to propose our Auditing Cloud-Hosted SaaS to West Virginia Department of Transportation ("WVDOT" or "Client").

We understand that choosing a GRC platform to meet your Audit & Compliance needs and business requirements can be a daunting task. Features and functionality among current platforms are a given. The tipping point that positions one platform over another is the level of experience of their executive leadership, customer success, and technical teams, the ease of use of the platform, and a smooth and efficient implementation process. All of these attributes make a service provider relationship that creates tangible value.

Thank you for this opportunity to present our RFQ response to become the Internal Audit Tool for WVDOT. If you have any questions, please do not hesitate to contact me as your account executive.

*Per Section 21 of your instruction to vendors, if awarded and you are going to publish our proposal to a public website, we are more than happy to provide a redacted version.

Yours sincerely,

Sean Mergenthal
Account Executive
smergenthal@auditboard.com
856.381.7892

TABLE OF CONTENTS

Per your request, the following documents have also been filled out and returned to you:

- CRFQ DOT23_145 Addendum 01
- CRFQ DOT23_145 Exhibit A Pricing Page Auditing SaaS RFQ
- CRFQ DOT23_145 General Terms and Conditions
- CRFQ DOT23_145 Software as a Service Addendum
- CRFQ DOT23_145 Specifications (doc)
- Final CRFQ_0803_DOT2300000145_2_WV_CRFQ_FORM

Solution Pricing and Services

The Future of Audit, Risk, and Compliance.

Elevate your teams with the most user-centric, efficient, and collaborative platform on the market.

	Plan License Metric	Stakeholder Users
OpsAudit	Features + Core Users	Unlimited

AuditBoard's scalable pricing is made up of an annual subscription fee and a one-time implementation fee.

➜ Pricing plans based on need and maturity

➜ Flexibility to choose the best solution or combination of solutions

➜ All Solutions include:

◆ **Unlimited data** storage in the application

◆ **Automatic updates** & **feature enhancements**

◆ **Top-rated technical support** and response times

◆ Access to **AuditBoard Academy** & **Support Center**

◆ Access to **AuditBoard Community**

◿ OpsAudit Plan

Solution Capabilities	Enterprise
Audit Forms	✔
Audit Project Management	✔
Audit Issue Management (Standard)	✔
Inventory / Auditable Entities	✔
Document Requests & Surveys	✔
Word-Based Audit Reports	✔
Timesheets	✔
Work Step Preparer Digest	✔
Audit Universe Risk Assessment (Standard)	✔
Audit Universe Risk Assessment (Custom)	✔
Risk-Based Audit Frequencies	✔
Microsoft Office Add-in	✔
Audit Issue Management (Custom)	✔
Audit Planning	✔
Resource Planning	✔
File & Workpaper Approval	✔

Platform Capabilities	Enterprise
AuditBoard Intelligence (ABI Dashboards)	✔
Reports Module	✔
WorkStream (Standard)	✔
Integrations - Standard	✔
Rest API	✔
Required Fields	✔
Reports API	✔
WorkStream (Custom)	✔
WorkStream Recurrence	✔
WorkStream Conditional Questions	✔
Integrations - Project Management	✔
Integrations - SSO Pack	✔
Integrations - Testing Automation	✔
Integrations - Analytics Database Access	✔
Integrations - Continuous Monitoring	✔
Integrations - Automated Evidence Collection	✔
Automated User Provisioning (SCIM API)	✔
Sandbox	✔

Pricing and Usage	Enterprise
Annual Subscription Fee (starting at)	**$119,000**
Core Users	15
Number of Audits	1,500
Included Integration Workflows (Automation)	100
Included Integration Monitors (Automation)	50
Price per additional Core User (Upon Signing Contract)	$4,500
Stakeholders	Unlimited

Implementation	Enterprise
One-time Implementation Fee - Standard	**$50,000**

** Enterprise subscription package only: 4 hours of virtual instructor–led training included. Additional training hours available for additional fee, subject to availability.

AUDITBOARD

RFQ Response for Auditing Cloud-Hosted SaaS (Technical Proposal)

SOLICITATION NO.:   CRFQ 0803 DOT2300000145

PRESENTED TO

Larry McDonnell, Senior Buyer

*Per Section 21 of your instruction to vendors, if awarded and you are going to publish our proposal to a public website, we are more than happy to provide a redacted version.

SALES ADVISORY TEAM

Sean Mergenthal, Account Executive
Chris Kane, Manager Product Solutions

June 28, 2023

AUDITBOARD

AuditBoard, Inc.
12900 Park Plaza Drive, Suite 200
Cerritos, CA 90703

June 28, 2023

West Virginia Department of Transportation
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Attn: Larry McDonnell

RE: AuditBoard RFQ response to WVDOT

Dear Mr. McDonnell,

On behalf of AuditBoard, Inc. ("AuditBoard" or "We"), we thank you for the opportunity to propose our Auditing Cloud-Hosted SaaS to West Virginia Department of Transportation ("WVDOT" or "Client").

We understand that choosing a GRC platform to meet your Audit & Compliance needs and business requirements can be a daunting task. Features and functionality among current platforms are a given. The tipping point that positions one platform over another is the level of experience of their executive leadership, customer success, and technical teams, the ease of use of the platform, and a smooth and efficient implementation process. All of these attributes make a service provider relationship that creates tangible value.

Thank you for this opportunity to present our RFQ response to become the Internal Audit Tool for WVDOT. If you have any questions, please do not hesitate to contact me as your account executive.

*Per Section 21 of your instruction to vendors, if awarded and you are going to publish our proposal to a public website, we are more than happy to provide a redacted version.

Yours sincerely,

Sean Mergenthal
Account Executive
smergenthal@auditboard.com
856.381.7892

TABLE OF CONTENTS

Per your request, the following documents have also been filled out and returned to you:

- CRFQ DOT23_145 Addendum 01
- CRFQ DOT23_145 Exhibit A Pricing Page Auditing SaaS RFQ
- CRFQ DOT23_145 General Terms and Conditions
- CRFQ DOT23_145 Software as a Service Addendum
- CRFQ DOT23_145 Specifications (doc)
- Final CRFQ_0803_DOT2300000145_2_WV_CRFQ_FORM

Executive Summary

Designed by industry professionals, AuditBoard's top-rated audit, risk, and compliance platform unlocks your team's potential and elevates strategic value.

Whether you are looking to simplify your SOX program, streamline internal audit, centralize risk management, or unify compliance management. AuditBoard provides the connectivity, efficiency, and flexibility you need to deliver on today's goals and tomorrow's vision.

We have thousands of audit, risk, and compliance professionals on our platform daily, from companies that went through the IPO process like TrueCar and TradeDesk to Fortune 500 companies including Walmart, Apple, and Intel. What these companies have in common is that they selected AuditBoard after exhaustive evaluation processes and extensive hands-on solution testing. AuditBoard is the top-rated GRC and audit management software on Gartner Peer Insights, G2.com, Capterra, and was recently ranked for the second year in a row as one of the 100 fastest-growing technology companies in North America by Deloitte.

AuditBoard Facts

Software comparison websites including G2, Gartner Peer Insights, and Capterra provide detailed reviews of AuditBoard by verified product users.
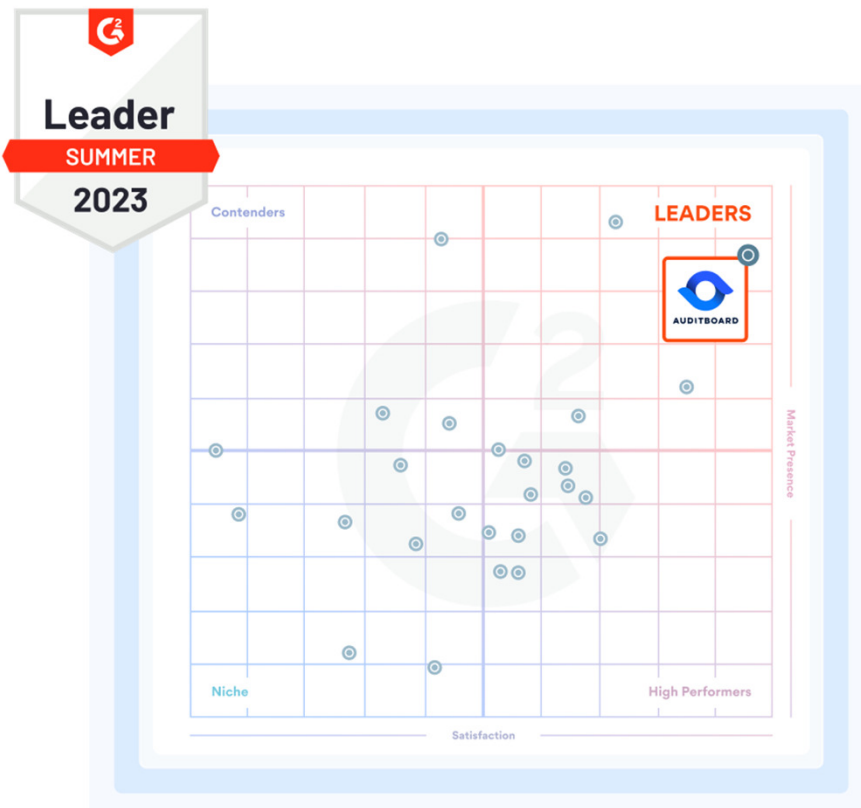
Audit Management Leader

AuditBoard User Ratings ★★★★½

9.3 Ease of Use
GRC Platforms Average: 8.5

9.2 Quality of Support
GRC Platforms Average: 8.9

8.7 Ease of Setup
GRC Platforms Average: 8.1

AuditBoard Facts

Deloitte's Technology | Fast 500 Ranking

AuditBoard was recently ranked for the third year in a row as one of the 100 fastest-growing technology companies in North America by Deloitte.

6

Companies from Fortune Top 10

Six of the Fortune Top 10 companies use AuditBoard to automate and streamline their audit department operations.

35%

Companies from Fortune Top 1000

30% of the Fortune Top 100 and Fortune 1000 companies use AuditBoard.

1800+

Companies that Use AuditBoard

The AuditBoard Platform is used by audit, risk, and compliance teams at over 1800+ companies.

1M+

Saved hours in 2022

AuditBoard clients collectively saved more than a million man hours in 2022.

98%

Renewal Retention

98% renewal retention among among AuditBoard clients.

The Modern Connected Risk Platform

- Free up teams to focus on the risks that matter
- Break down silos & embed risk awareness into the front lines
- Assess risk/value with more clarity and continuously recalibrate
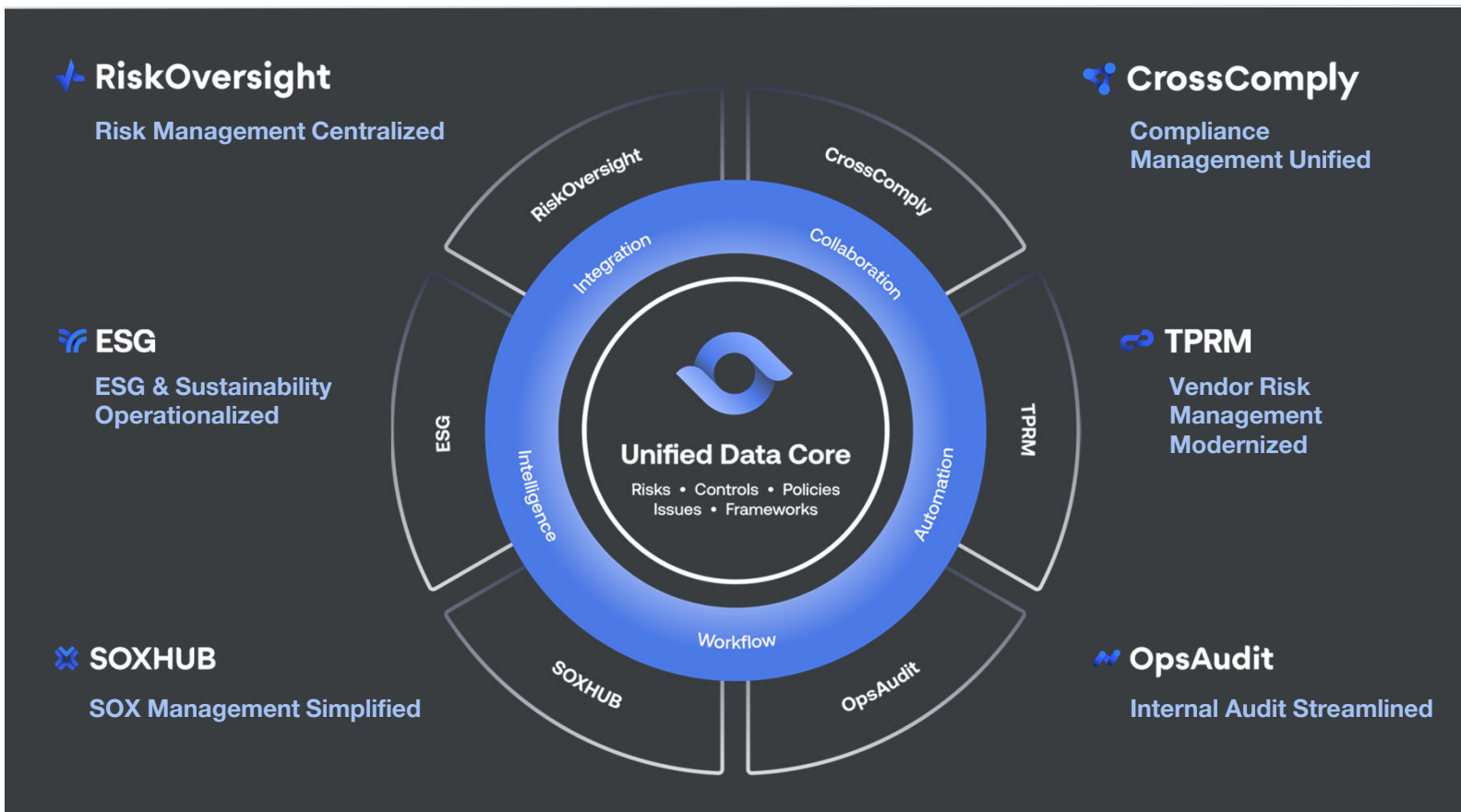
AuditBoard's top-rated connected risk platform unlocks your team's potential and helps you deliver more strategic value. Whether you are looking to simplify your SOX program, streamline internal audit, unify compliance management, or centralize risk management, AuditBoard provides the connectivity, efficiency, and flexibility you need to deliver on today's goals and tomorrow's vision.

⚠ **I#5 - Airfare Bookings - Days in Advance**   ○ **Open**

TESTER
Andrew Johnson

REMEDIATION OWNER
Barry Byrd

Identified By
Internal Audit

Identified Date
2022-09-30

Issue Description
Employee flights booked less than 7 days in advance, costing company approx $244k (based on average ticket prices).

Issue Severity
Medium

▶ Planning

▼ Fieldwork

⚠1 R1 Real-time, online data for instant... 2022-10-12 P JI R SS 💬 2

⚠1 ○ Duplicate Checks 2022-09-15 P JI R SS 💬 1

✓ User Access and Authorizations 2022-08-01 P JI R SS 💬 6

▶ Walkthrough/Understanding ▬▬▬▬▬▬▬ 83%

▶ Reporting ▭▭▭▭▭▭▭ 0%

OpsAudit

Internal Audit Transformed

- **Gain real-time visibility** into audit activities and findings. Automate audit committee reporting.

- **Add value** at every stage of the internal audit process from audit planning to fieldwork, testing, and reporting.

- **Centralize** documentation, audit procedures, evidence, findings, and prior year work.

Account Management Team

Your AuditBoard Team

The AuditBoard Team working on your account will have a high level of internal and external audit experience and can speak your language when it comes to understanding your environment's business requirements. This is true across our business development, product, and customer implementation and success teams.

SEAN MERGENTHAL **|** Account Executive, Enterprise

- Over 10+ Years of Internal Audit, SOX, and Risk experience
- PwC and EY
- CISA

CHRIS KANE **|** Product Solutions Manager

- 6+ years of SOX and External Audit experience
- Former PwC Manager
- Certified Public Accountant (CPA)

Staffing Strategy

■ Your Customer Success Team

Fast Implementation

With the fastest implementation process in the industry, get up and running in just a couple of months.

Experienced Onboarding and Customer Success Teams

The entire AuditBoard team is based in the United States. The Customer Success and Onboarding Teams working on your account bring a high level of SOX and audit knowledge, averaging 10-years of professional experience. We speak your language when it comes to understanding your obstacles and unique business requirements. The below team members are a representation of the caliber of team leads who will be staffed on the implementation project for WVDOT.

We anticipate the implementation team for WVDOT to be comprised of three (3) individuals, in addition to the team lead, who will work on the implementation and training for a period of six full-time weeks, considering all offerings in scope and the timing required by WVDOT.

Let Us Do the Heavy Lifting

Implementing a software solution does not have to disrupt your current operations. Our experienced onboarding team will perform most of the software set up - all we need from you is your current testing documentation, testing templates, reports, and a couple hours each week for a status update call.

CHRIS ROTANTE | Director of Implementation

- Background in finance & accounting
- 6+ years Big 4 experience including both KPMG & PwC
- Specialized in SOX IT audit, internal audits, SOC1 reviews, cybersecurity reviews, & BCP/DR

ANNA FRY | Director of Implementation & COE

- 10 Years+ of SOX & Internal Audit Experience
- Experience includes SOX, Internal Audits, Enterprise Risk, and Compliance at KPMG
- High level of expertise in SOX and operational audits

EMMA KONG | Director of Implementation

- 8+ Years of Internal and External Audit experience
- 4 years of system implementations experience
- Onboarded 100+ OpsAudit customers including top Fortune 500 companies

Appendix A | **Technology & Security**

Appendix A

Technology & Security

AuditBoard was built by industry experts. It's our shared mission to improve your organization's risk and compliance posture. That's why we design our products with industry leading security practices and multiple layers of security controls that ensure security, confidentiality, integrity and availability for our customers and their data.

- Industry leading secure cloud-based architecture
- Robust and customizable access controls
- Data encryption in transit and at rest
- Designed for performance, scalability and resilience
- Integration ready with SAML support for SSO and two-factor authentication
- Focus on industry standards and compliance

For more information about AuditBoard's technology and security, please visit auditboard.com/technology-security.

Scan QR code to learn more.

Appendix B

REVIEWS

Peer Reviews for AuditBoard:

- **G2**: https://www.g2.com/products/auditboard/reviews

- **Gartner**: https://www.gartner.com/reviews/market/audit-management-solutions/vendor/auditboard/product/auditboard

- **Capterra**: https://www.capterra.com/p/148230/SOXHUB/

Summary of Similar Projects:

- Estee Lauder: https://www.auditboard.com/blog/estee-lauder-success-story/

- Eagle Materials: http://go.auditboard.com/rs/961-ZQV-184/images/Case-Study-Eagle-Materials-CS.pdf

- Additional Customer Success Stories: https://www.auditboard.com/customer-success/

Customer Quotes:

Emily Williams, Sr. Manager, Global Audit Services, Walmart
"We implemented AuditBoard in 2018 and the implementation process went very smoothly. We have now been using AuditBoard for 8 months now and have had an amazing experience. Customer service continues to be responsive and quickly addresses our needs. The tool is very user friendly, and our audit team collectively agrees that it exceeds our previous tool in nearly every way."

Michael Stowers, Vice President, Internal Audit, Eagle Materials
"Audits that would typically take us 150 hours, we were completing in 100 hours. The same went for our fieldwork: each week, we were able to put a bow on it, and it didn't carry over to the following week"

Appendix B

Solution Benefits of ROI

Measurable Business Impact and Savings. AuditBoard will fundamentally improve daily operations and increase the strategic value your department can provide to the organization. Because the AuditBoard Platform is predicated on intuitive use, rapid implementation, and providing users with solutions they can use instinctively; you'll experience significant increased efficiencies and associated cost-savings.

UNITED BANK

"After year 1, our Department will be saving approximately 35% a year If every one of our 26 auditors save just 1 minute a day due to this, we've gained over 108 audit hours in a year!"

Courtney Sheff, Senior IA Manager

EM Eagle Materials

"Audits that would typically take us 150 hours, we are now completing in 100 hours."

Michael Stowers, Vice President, Internal Audit

Waters

"We re-deployed 1000 hours annually from administrative planning efforts to added value tasks and 120 hours quarterly on completing certifications."

Shannon Murray, Manager, Internal Audit

ALLEGRO microsystems *INNOVATION WITH PURPOSE*

"If we didn't have AuditBoard today, I think we'd need two more junior staff people just to manage the admin tasks — in a team of 20-25, that's 10% more."

Erich Manz, Corporate Controller

Post

"We used pretty conservative estimates, and found that within the first year we recouped our investment."

Andrew Ganey, Director of Internal Audit

Altra Motion

"I'd estimate that just in terms of providing reconciliation information to our external auditor, implementing AuditBoard has saved us anywhere from a half to three quarters of an FTE worth of time."

Alex Chin, Director of Internal Audit

SOLICITATION NUMBER: CRFQ DOT2300000145
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[   ]   Modify bid opening date and time

[   ]   Modify specifications of product or service being sought

[✓]   Attachment of vendor questions and responses

[   ]   Attachment of pre-bid sign-in sheet

[   ]   Correction of error

[   ]   Other

Description of Modification to Solicitation:

To attach vendor questions and responses.

Bid opening remains June 28, 2023 at 1:30PM Eastern Time

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ DOT23000000145
Auditing SaaS RFQ - Technical Questions

Question 1

Can you please provide high-level detail around the types of audits per year, such as Financial; Performance; Compliance; IT?

Response 1

Refer to specification: 4.1.1.1 regarding the capacity requirements for audit files. Note there is none specified to the types of audit engagements and 4.1.1.4 regarding the flexibility of the program to create workpapers, audit programs, reports and templates for use.

Question 2

Are there any testing templates (aka audit programs) currently in place to streamline the process for each type of audit? If so, how many?

Response 2

Refer to specification: 4.1.1.4 regarding the flexibility of the program to create workpapers, audit programs, reports and templates for use.

Question 3

How many unique final report/opinion templates do you use?

Response 3

Refer to specification: 4.1.1.4 regarding the flexibility of the program to create workpapers, audit programs, reports and templates for use.

Question 4

Do you need any capabilities around audit risk assessments (either at the audit plan level or individual audit)?

Response 4

Refer to specification: 4.1.1.4 regarding the flexibility of the program to create workpapers, audit programs, reports and templates for use.

Question 5

> Are controls tested or documented during audit processes? If yes, how many? How many would need to be pre-loaded for implementation?

Response 5

> Refer to specification: 4.1.1.4 regarding the flexibility of the program to create workpapers, audit programs, reports and templates for use.

Question 6

> Do you need any capabilities around tracking audit findings, action plans, and remediation status? If so, how many audit findings and action plans would need to be pre-loaded for implementation?

Response 6

> Refer to specification 4.1.1.2. for the capability to create and maintain a library of findings and create templates by individual client or engagement. Note no quantity specified.

Question 7

> Do you have more than one (1) final slide deck/presentation that you want setup as part of the implementation? If yes, please confirm and indicate how many? For example, sometimes audit management teams request the setup of one (1) quarterly audit committee slide deck during implementation, in addition to other slide decks/presentations that require separate templates.

Response 7

> Refer to spec 4.1.1.28 for capability of the software to provide data information in report format.

Question 8

> Does the Agency have a specific control framework(s) (e.g., COSO or Greenbook) they follow to populate the control library?

Response 8

> No.

Question 9

> Section 4.1.1.2 is the first section that uses the term "client". Can you explain this term and indicate whether this is a related or unrelated party to the State of West Virginia's Department of Transportation?

Response 9

This specification refers to the software capability or flexibility for the finding's library and template creation and organization. The specifications do not define a client on purpose as it will be variable.

Question 10

Section 4.1.1.3 mentions "automated integration workflows" and "automated integration monitors". Can you explain these terms or provide examples?

Response 10

Automation integration workflow is a unit of automation that will pull evidence from another system, (eg; wvOASIS (ERP)).

Automated Integration Monitors are a workflow that will run automated tested procedures defined by WVDOT.

Question 11

Can you provide any details on the macros mentioned in Section 4.1.1.21?

Response 11

Vendors must meet 4.1.1.21 specification to allow the full functionality of using Microsoft Office Suite Software.

Question 12

Can you provide any details on the interfaces mentioned in Section 4.1.1.31?

Response 12

Refer to specification 4.1.1.31. , vendors proposed system must have the ability for end-users (WVDOT) to configure reporting dashboards straightforward without the need for vendor support or enchantment.

Question 13

Can you provide any details on the scope of integration required by Section 4.1.1.33?

Response 13

Refer to specification 4.1.1.33, vendors proposed solution must integrate with agency-owned Microsoft Power BI report and visualization software.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ DOT23*145

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.

AuditBoard, Inc.
_____
Company

Tina Yeh
EF911F3B9A6241C
_____
Authorized Signature

6/20/2023
_____
Date

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

EXHIBIT A - PRICING PAGE - CRFQ DOT23*145

										AuditBoard Notes
Auditing Cloud-Hosted SaaS RFQ (81230134)										
LOCATION: BUILDING 5, ROOM A-720, CHARLESTON, WV 25305										
Contract Item Number	**Description***	**Unit of Measure**	**Estimated Quantity***	**Year One Unit Cost**	**Optional - Year Two Unit Cost**	**Optional - Year Three Unit Cost**	**Optional - Year Four Unit Cost**	**Optional - Year Five Unit Cost**	**Extended Cost**	Current listed cost is for the current description. As licenses or other metrics increase, pricing may deviate.
Auditing Cloud-Hosted SaaS Subscription / License										
4.1.1, 4.1.2, 4.1.1.2.	Enterprise SaaS Subscription - Must at a minimum include 25 core user licenses, 1500 audits anually, 100 integration workflows (automation) annually, 50 integration monitors (automation) anually and unlimited stakeholders	LS	1	$164,000.00	$164,000.00	$164,000.00	$164,000.00	$164,000.00	$820,000.00	
4.1.1, 4.1.2, 4.1.1.2.1	Enterprise SaaS Subscription Per Additional Core User (per license)	EA	1	$5,400.00	$5,400.00	$5,400.00	$5,400.00	$5,400.00	$27,000.00	Additional cose per license is $5,400. Discounts may be discussed depending on volume
Auditing Cloud-Hosted SaaS Services**										
4.1.3.1	Initial Cloud-Hosted SaaS Implementation Fee (lump sum)	LS	1	$50,000.00					$50,000.00	
4.1.3.2	Initial Cloud-Hosted SaaS Virtual Instructor Led Training (hourly rate)	EA	4	$0.00					$0.00	Included with subscription
4.1.3.3	Virtual Instructor Led-Training (hourly rate)	EA	25	$250.00	$250.00	$250.00	$250.00	$250.00	$31,250.00	Go through the initial training and onboarding - many customers feel they dont need this.
4.1.3.4	Virtual Adminstrator Training (hourly rate)	EA	25						$0.00	Included with subscription as a self service option with AuditBoard academy. You also have access to a dedicated Customer Success Manager who can train you to use that platform that is included in the subscription.
4.1.3.4	On-Site System Adminstrator Training (hourly rate)	EA	25	$250.00	$250.00	$250.00	$250.00	$250.00	$31,250.00	
4.1.5	Cloud-Hosted SaaS Professional Services Support On-Site Rate (hourly rate)	EA	25	$250.00	$250.00	$250.00	$250.00	$250.00	$31,250.00	
4.1.5	Cloud-Hosted SaaS Professional Services Support Virtual Rate (hourly rate)	EA	25						$0.00	Unlimited and included with subscription
						Total Overall Cost:			$990,750.00	

* The estimated purchase volume for new licenses represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

**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. Location: 1900 Kanawha Boulevard E. Building 5, Charleston, WV 25305

***Optional Renewals- Year Two through Year Five may be renewed by Change Order upon mutual agreement between the Vendor and Agency.

Sean Mergenthal Electronic signature - 6/28/23

Vendor Signature

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.

Revised 11/1/2022

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 _____
_____ . 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 _____ 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.

[ ]

[ ]

[ ]

[ ]

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: _____ 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: _____ 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 http://www.state.wv.us/admin/purchase/privacy/default.html.

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.

Revised 11/1/2022

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.

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) _____

(Address) _____

(Phone Number) / (Fax Number) _____

(Email address) _____

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.

_____
(Company)

_____
(Signature of Authorized Representative)

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

_____
(Phone Number) (Fax Number)

_____
(Email Address)

Software as a Service Addendum

1. Definitions:

<u>Acceptable alternative data center location</u> 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.

<u>Authorized Persons</u> 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.

<u>Data Breach</u> 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.

<u>Individually Identifiable Health Information</u> 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.

<u>Non-Public Data</u> 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.

<u>Personal Data</u> 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).

<u>Protected Health Information (PHI)</u> 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

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

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

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: _____ _____

<u>SPECIFICATIONS</u>

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. Vendor must provide, upon request, documentation showing their experience with having successfully completed implementation of an existing Auditing Cloud-hosted Saas with workflows within an organization of similar size and complexity or larger thanWVDOT.
   Upon further request, we are more than happy to provide documentation. We work with a large range of clients across different industries as well as organization size, from pre-IPO companies all the way to Fortune 10. Our solution is scalable and works well across different industry verticals. Our clients are utilizing AuditBoard for a variety of modules, from SOX compliance to audit management. AuditBoard has over 1,800+ clients and is the top rated audit management solution on the market. Current clients utilizing our audit management solution include Walmart, United Bank, Lockheed Martin, BlackRock, Apple, Ralph Lauren, CVS, Intel, Party City, Miami Dade county, and many more including many more state run and public entities.

   3.2. Vendor must provide, upon request, proof as an authorized reseller of the proposed Auditing Cloud-hosted Saas or a Sole Source letter if the Cloud-hosted Saas is proprietary to the vendor before contract award.
   Confirmed. Upon further request, we can provide proof.

   3.3. Vendor must provide, upon request, proof their proposed solution is ISO 27001 certified (SOC-2).
   Both documents can be provided upon further request.

4. GENERAL REQUIREMENTS:

4.1. Mandatory Contract Item Requirements: The Vendor shall provide Agency with the Contract Items listed below. Contract Items must meet or exceed the mandatory requirements listed below.

4.1.1. General Auditing Cloud-hosted Saas Operating Requirements

4.1.1.1. Cloud-hosted Saas must have the capability to store hundreds of audit files per fiscal year.

AuditBoard allows for unlimited data usage and for any file type or file size to be uploaded to the system.

4.1.1.2. Cloud-hosted Saas must include a subscription for up to a minimum of twenty-five (25) users in the audit work papers system concurrently from multiple locations, allow for at least one thousand five hundred (1500) audits annually, allow at least one hundred (100) automated integration workflows annually, allow at least fifty (50) automated integration monitors annually and must include unlimited stakeholders.

AuditBoard's Enterprise package offers 25 Core Users (i.e. Auditors), and unlimited stakeholder user licenses (i.e. Auditees) with the annual subscription. Specified numbers of audits, workflows, and monitors can all be accommodated by the enterprise level subscription.

4.1.1.2.1. Cloud-Hosted Saas must have the ability to add additional core user licenses as requested and purchased by the Agency.

WVDOT will have full access over user maintenance to add, edit, or delete users.what was

4.1.1.3. Cloud-hosted Saas must have the capability for the client to create work papers, audit programs, reports, and templates for use.

During implementation, our onboarding team will work with you to set up any templates, including audit program steps. In addition, a sub-set of end users (e.g. methodology team) will be trained to create and edit master templates on a go-forward basis. These may be imported to an audit step at the creation of the audit or ad hoc.

4.1.1.4. Cloud-hosted Saas must filter work papers by client, engagement type, fiscal year, or by auditor.

AuditBoard is highly configurable, where data fields, workflows, views, dashboards and reports can be configured by the end user. Client, engagement type, fiscal year, and auditor can be configured within our list views.

4.1.1.5. Cloud-hosted SaaS must support and integrate with agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu (PDF) programs for searching, retrieval and saving of documents.

AuditBoard offers a full integration with Microsoft Office suite (i.e., Excel,

PowerPoint, Word, and Visio), Google, Lucidchart, and PDF that enables our clients to generate documents in their preferred format. Documents can be edited on the platform directly or downloaded onto native format, based on client preferences.

4.1.1.6. Cloud-hosted Saas must be compatible with states Google email system.

Confirmed.

4.1.1.7. Cloud-hosted Saas must have the ability to assign hierarchy of roles for users.

Roles are always granted on the theory of least-privileged access, and only after being formally requested and approved by management.

4.1.1.8. Cloud-hosted Saas must have the capability of add/alter client information, auditors, approvers, reviewers, and administrative personnel.

Client will have visibility to review and export user access listings. System administrators will be trained to add, remove, or adjust user access as appropriate. Additionally, AuditBoard includes unlimited customer support to assist with any updates.

4.1.1.9. Cloud-hosted Saas must be able to create assignments to specific users.

Confirmed. Assignments and tasks (e.g. document requests) can be provided to individual users within the platform.

4.1.1.10. Cloud-hosted Saas must have the capability to retrieve prior audit information from agency owned Teammate Software. This information would reference prior completed set of working papers for a particular entity.

Due to the proprietary nature of audit software, AuditBoard would not be granted access to Teammate's audit software nor would Teammate ever be granted access to AuditBoard. For customers using any existing system, clients are responsible for extracting their own data and migrating the data into AuditBoard templates. We have hundreds of customers who have migrated over from Teammate and the templates will provide instruction on how to populate the data.

4.1.1.11. Cloud-hosted Saas must have the capability to convert past audit work papers from agency owned current TEAMMATE software.

Once data is initially extracted from Teammate and provided to us within the AuditBoard templates, AuditBoard handles the upload process for your current year audit plan and any outstanding issues. Prior fiscal year audit data for engagements and issues that have been fully closed will be uploaded to the perm files section in their original formats (excel, pdf etc.) for reference.

4.1.1.12. Cloud-hosted Saas must allow users have the capability to view, alter and create multiple workpapers at the same time.

Coarse grained authorization in the AuditBoard platform is based on RBAC (role-based access control). Fine grained authorization is

determined by specific assignments within the platform, or ABAC (attribute-based access control). The combination of these access control mechanisms allows clients to have full control over how data is accessed and permissioned within the platform.

4.1.1.13. Cloud-hosted Saas must have evidence of workpaper completion and review by whom and the date completed.

> Confirmed. Each working paper has its own workflow including tester and reviewer sign-offs. All sign-offs are marked with a timestamp and responsible individual. Once a staff has signed off on the working paper, the Manager / Director will receive automated email and platform notifications, which indicate the working paper is ready for review. Status of workpapers drives real-time dashboards.

4.1.1.14. Cloud-hosted SaaS must have controls over workpaper sharing and have the capability for different employees to alter same work paper.

> Workpapers are maintained electronically within the platform. During implementation, our onboarding team will work with you to set up any templates you may need. In addition, a sub-set of end users (e.g. methodology team) will be trained to create and edit templates on a go-forward basis as well.

4.1.1.15. Cloud-hosted Saas must allow peer review team to view work papers.

> Confirmed. Each working paper has its own workflow including tester and reviewer sign-offs. All sign-offs are marked with a timestamp and responsible individual.

4.1.1.16. Cloud-hosted Saas must have the capability to leave reviewer comments notes for work paper corrections that can be removed by reviewer.

> AuditBoard has fully integrated Commenting functionality available throughout the platform which allows users to tag each other and even tag entire teams. Notes or comments can then be removed or permissioned off to only be visible to certain roles.

4.1.1.17. Cloud-hosted Saas must have indicators that work papers have been altered and needs reviewed.

> Confirmed. Each working paper has its own workflow including tester and reviewer sign-offs. All sign-offs are marked with a time-stamp and responsible individual. Once a staff has signed off on the working paper, the Manager / Director will receive automated email and platform notifications, which indicate the working paper is ready for review. Frequency and content of email notifications may be configured based on your needs (e.g. daily digest, weekly digest, etc.).

4.1.1.18. Cloud-hosted Saas must have the capability to reference or link support documentation.

> Confirmed. AuditBoard has a full integration with the Microsoft Office Suite and Adobe PDF which allows end users to continue

using the applications and functionality they are used to using today. All uploaded files include hyperlinks which may be inserted throughout the platform for quick and easy reference. Any external URLs (e.g., your share drive protected by a firewall) may be referenced and click-able within the platform, as well.

4.1.1.19. Cloud-hosted Saas must automatically generate audit reports to agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu with indicators of each engagement in progress.

Confirmed. Audit issues can be linked within audit reports. By utilizing an audit report template, you can automatically pull issues into your final audit report with a drag and drop capability for prioritizing audit issues. Reports generated will include the latest status of the audit issue and remediation plan. Templates can be configured based on customer preference.

4.1.1.20. Cloud-hosted Saas must have the capability to run macros in agency owned Microsoft Office Suite software while in the audit Cloud-hosted SaaS system.

AuditBoard offers a full integration with Microsoft Office suite (i.e., Excel, PowerPoint, Word, and Visio) and Adobe PDF that enables our clients to generate documents in their preferred format. Documents can be edited on the platform directly or downloaded onto native format, based on client preferences.

4.1.1.21. Cloud-hosted SaaS must have the capability to lock down work papers and have the capability of removing this lock this if necessary.

AuditBoard is a fully role based platform with granular permissions functionality. Permissions can easily be set for workpapers or projects that need to be locked down to a small subset of users.

4.1.1.22. Cloud-hosted Saas must have the capability to access multiple clients working files at the same time.

Confirmed.

4.1.1.23. Cloud-hosted Saas must have the ability to spell and grammar-check text fields.

Confirmed. Given AuditBoard is a web-based application, spell check would work There is a spell check that comes with chrome/the Internet Browser.

4.1.1.24. Cloud-hosted Saas must have the capability to store client files on an external hard drive.

N/A - Everything is hosted in the cloud. AuditBoard is a SaaS cloud-based platform hosted on AWS (Amazon Web Services). AuditBoard leverages core AWS services with multi-availability zone configurations (EC2, RDS, S3). All data on our private and public networks are always transported via encryption. We use

TLS 1.2 to encrypt data in transit and AES-256 to encrypt all customer data at rest.

Cloud-hosted Saas must have the capability to tick mark or reference agency owned Acrobat Adobe Professional or Bluebeam PDF software. AuditBoard has a full integration with the Microsoft Office Suite and Adobe PDF which allows end users to continue using the applications and functionality they are used to using today. All uploaded files can be hyperlinked to one another, which may be inserted throughout the platform and within documents for quick and easy reference. Also, our embedded document and spreadsheet editors allow full Rich Text editing.

4.1.1.25. Cloud-hosted Saas must have indicators that work paper has been changed after reviewer sign off.

AuditBoard includes a complete audit log of all changes made in the platform. Each record in the log includes a date and timestamp as well as who made the change. Each working paper has its own workflow including tester and reviewer sign-offs. All sign-offs are marked with a timestamp and responsible individual. Once a staff has signed off on the working paper, the Manager / Director will receive automated email and platform notifications, which indicate the working paper is ready for review. Status of workpapers drives real-time dashboards.

4.1.1.26. Cloud-hosted Saas must have the capability to run reports to compile data information such as number of audits completed, number of audits in progress, number of findings issued, audit hours per engagement, audit hours per auditor, audit hours per fiscal year for a section and for entire Division.

All data points can be displayed in our dashboards and reports, which can be filtered to slice and dice all aspects of your audit plan completions, including individual or aggregate audit progress, hours, findings, and more.

4.1.1.27. Cloud-hosted Saas must have a dedicated audit workflow process and pages for each audit with configurable sections for planning, fieldwork, reporting, etc in a straightforward to navigate user interface.

AuditBoard supports full audit lifecycle management from planning, fieldwork and reporting. Testing can be organized and configured into test phases. Real time dashboards allow for progress tracking and the solution has the ability to send out automated reminders. AuditBoard was developed by auditors for auditors and is purpose-built to work the same way auditors think and act. As such, the application is intuitive and easy to use.

4.1.1.28. Cloud-hosted Saas must provide the ability for end-users to configure

reporting dashboards straightforward without the need for vendor support or enchantment.

Users have the ability to configure custom dashboards and reporting with PowerBI. Additionally, a Reports module allows you to build any additional custom reports.

4.1.1.29. Cloud-hosted Saas must provide the ability for WVDOT to update configuration of interface key field names, layout and attributes without requiring vendor assistance.

> AuditBoard is highly configurable, where data field labels, workflows, views, dashboards and reports can be configured by the end user.

4.1.1.30. Cloud-hosted Saas must accommodate any file size or file type with very small data load latency issues.

> AuditBoard accepts any file type without size restrictions. Latency is not a measure of the application. Latency is a measure of the distance of the user to the service. Impact of latency on user experience is a function of the users tolerance relative to the performance of the application. We have global users of the AuditBoard service who experience upwards of 300ms.

4.1.1.31. Cloud-hosted Saas must integrate with agency-owned Microsoft Power BI report and visualization software.

> AuditBoard Intelligence (ABI Dashboards) powered by our integration with Microsoft Power BI, provides user-friendly and real-time dashboarding and data visualizations. Users can customize and configure dashboards to reflect their reporting requirements. These dashboards enable users to build visualizations, report on desired metrics, and allow for trend insights / analysis.

4.1.2. **Auditing Cloud-hosted Saas Security Requirements**

4.1.2.1. Cloud-hosted Saas Servers must be replicated and load-balanced across data centers and regions.

> The AuditBoard application is a single page app that require initial load of assets and then incremental web service calls to function properly. This architecture is designed to auto-scale based in load and functions effectively on any bandwidth. We maintain no minimum bandwidth requirements to function properly. We have redundancy across our entire stack and rely on managed services provided by AWS, which each have their own built-in redundancy.

4.1.2.2. Cloud-hosted Saas must take real-time backups, continuously, that allow for data recovery at one second intervals.

> Database backups are made every 24 hours and kept in storage for 35 days. Backups of your database instance will be taken before version upgrades and before your yearly archive. Additionally, all database transactions are logged continuously allowing for recovery at 1-second granularity.

4.1.2.3. Cloud-hosted Saas must save daily encrypted database backups that are also stored in encrypted, redundant, and versioned storage.

AuditBoard relies on Amazon Web Services (AWS) infrastructure to manage backups and system availability. All data is continuously backed up to s3 Storage with 1-sec granularity. Full database backups are made every 24 hours and kept in storage for 35 days using versioned S3 storage. All AuditBoard client data backups are stored in Amazon S3 storage with multi-datacenter redundancy. This storage is encrypted at rest and physically secured inside Amazon's data-centers.

4.1.2.4. Cloud-hosted Saas must have built in redundancies at the regional, datacenter, hardware, container, and data levels.

The AuditBoard architecture was designed for redundancy and high-availability:

Hardware Redundancy - All components leverage AWS services with multi-availability zone configurations (EC2, RDS, S3).

Regional Redundancy - Production resources are primarily hosted in the US-WEST-2 AWS Region (Oregon). US-EAST-1 (Virginia) is considered the failover region in the case of a full US-WEST-2 regional failure.

Container Redundancy - In the case of a container (pod) failure or host (node) failure, Kubernetes will automatically restart and reschedule the Container onto a new host.

Data Redundancy - All data is continuously backed up to S3 with 1-sec granularity. Full database backups are made every 24 hours and kept in storage for 35 days using versioned S3 storage.

4.1.2.5. Cloud-hosted Saas must be able to export all data and files to common formats such as CSV.

End users have the ability to export all data from AuditBoard in standard formats (ZIP, PDF, CSV, etc.). Details of the format types are as follows:
Controls: Excel, CSV, PDF
Narratives: PDF
Test-Sheets: Excel, JSON
Workpapers and attachments: original file format (Word, Excel, PDF, etc.)
Flowcharts: PDF and original file format (e.g. Visio)

4.1.2.6. Cloud-hosted Saas must be accessible and have full functionality from web browsers (eg: Chrome, Edge Firefox)

We support all operating systems, all you need is an internet browser to connect to our platform. We are best optimized on the following versions: Google Chrome (40+), Microsoft Internet Explorer (11+), Microsoft Edge, Apple Safari (8+), Mozilla Firefox (38+).

4.1.2.7. Cloud-hosted SaaS servers must have 24/7/365 physical security monitoring.

The physical and environmental security controls for the

organization's production environments are carved out and the responsibility of AWS. From AWS "We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses."

4.1.2.8. Cloud-hosted Saas must have single sign-on ability and work with State owned Active Directory.

AuditBoard supports Single Sign-On through SAML 2.0, which allows for integration with Active Directory (ADFS), Azure Active Directory, Okta, OneLogin, Google Apps, SiteMinder, Ping and more. We also support multi-factor authentication.

4.1.2.9. Cloud-hosted Saas must have an out of the box role-based pennission(s) or allow for custom roles to restrict what can be viewed or edited down to field level.

Coarse grained authorization in the AuditBoard platform is based on RBAC (role-based access control). Fine grained authorization is determined by specific assignments within the platform, or ABAC (attribute-based access control). The combination of these access control mechanisms allows clients to have full control over how data is accessed and permissioned within the platform.

4.1.2.10. Cloud-hosted SaaS must have the ability for two-factor authentication.

Two factor authentication is required for any access, on-site or remotely, to the company assets.

4.1.2.11. Cloud-hosted Saas must have data protection and at a minimum have end-to-end TLS 1.2 encryption or better.

All data in transport uses TLSv1.2 for encryption.

Please see attached, 'Data Security Policy'.

4.1.2.12. Cloud-hosted Saas must have storage encryption and protect all WVDOT auditing files, databases and backups with at least AES-256 bit encryption or better before being written to permanent disk storage.

AuditBoard utilizes AES-256 Encryption for data at rest (on disk).

4.1.2.13. Cloud-hosted Saas must have data integrity features and protect WVDOT's data from loss, manipulation, or corruption by at a minimum using cryptographic hashing controls that enforce versioning and provide secure transactional abilities.

The application contains business logic that validates data before and/or after queries are executed to ensure the integrity of the data submitted. All database change transactions are done using parameterized queries and TLS to secure the transmission of data.

Secure tokens are used to authenticate each session. Customer files are stored encrypted in AWS S3, with versioning enabled. The S3 native integrity checking mechanisms are used to ensure file integrity.

Since we are a SaaS application, we cannot enforce DLP on a customer's network or endpoints. We do however enforce DLP Protection on our own internal services (like on employee devices, and enterprise communications applications). Customers should consider enforcing DLP within their own environment or consider limiting the ability to export data to particular roles within the application. We also offer IP whitelisting to only allow connections from a customer's network.

4.1.2.14. Cloud-hosted SaaS must use NIST-compliant data sanitization procedures to securely delete data requested by WVDOT that has reached the end of use life.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.

4.1.2.15. Cloud-hosted Saas audit trails must be strictly monitored to ensure performance, availability, and security.

The following systems are used for logging and security monitoring: LogDNA, Stackrox, Signal Sciences, CloudWatch, CloudTrail, GuardDuty, Azure performance/utilization tools, and Rollbar.

AuditBoard maintains full audit log of all login attempts into our systems. AuditBoard also maintains a full audit log of changes made to WVDOT's data. These audit logs are available to WVDOT 24/7/365. Access to the audit logs is fully permission-able, the WVDOT can decide who has access to the audit logs.

4.1.2.16. Cloud-hosted Saas audit trails must have audit logs that track every data change made in the system against an authenticated user.

Our platform maintains a full audit log of all changes that are made. End users may revert back to previous versions of documents to resolve any conflicts.

4.1.2.17. Cloud-hosted Saas audit trail must have every successful or failed attempt to access WVDOT Saas Cloud-hosted instance. This data must be recorded and viewable by WVDOT/WVOT.

AuditBoard maintains full audit log of all login attempts into our systems. AuditBoard also maintains a full audit log of changes made to WVDOT's data. These audit logs are available to WVDOT 24/7/365. Access to the audit logs is fully permission-able, the WVDOT can decide who has access to the audit logs.

4.1.3. **Training & Implementation**

4.1.3.1. Vendor must implement, configure, build and setup proposed cloud-hosted Saas for WVDOT.

Confirmed. An average implementation takes 10 weeks (regardless of modules). Start date is defined as the day Customer provides their documentation and end date is go-live date which marks the end of user acceptance testing (UAT). AuditBoard's responsibilities are to configure the system to be ready for use, it is the Customer's responsibility to test the system. We generally support Customers for 4 weeks during the UAT period.

4.1.3.2. Vendor shall provide the Agency with virtual training within five (5) working days of Cloud-hosted Saas implementation.

All Customers will have access to AuditBoard Academy (ABA), our online training portal after contract sign.

Customers with Enterprise subscriptions also have 4 hours of virtual Instructor Led Training (vILT) and can choose from a course catalog.

4.1.3.3. Vendor shall provide on-going training rates for virtual instructor led training.

All Customers will have access to AuditBoard Academy (ABA), our online training portal after contract sign. Customers with Enterprise subscriptions also have 4 hours of virtual Instructor Led Training (vILT) and can choose from a course catalog. 4 hours of custom training led by a professional trainer. Customers can choose from a course catalog for up to 4 hours of lessons. Courses vary in length, generally 1 to 2 hours per course. The trainings are tailored to the customer's environment and are conducted virtually. The trainings are recorded for playback and distribution.

4.1.3.4. Vendor shall provide on-going training rates for virtual and on-site administrator training.

Our training is typically done remotely.

All Customers will have access to AuditBoard Academy (ABA), our online training portal after contract sign. Customers with Enterprise subscriptions also have 4 hours of virtual Instructor Led Training (vILT) and can choose from a course catalog. 4 hours of custom training led by a professional trainer. Customers can choose from a course catalog for up to 4 hours of lessons. Courses vary in length, generally 1 to 2 hours per course. The trainings are tailored to the customer's environment and are conducted virtually. The trainings are recorded for playback and distribution.

4.1.4. Technical Support

4.1.4.1. Vendor shall provide technical support for the Cloud-hosted Saas utilizing a primary technical support phone number, ticket portal or primary technical support email address.

Support agents are available for support via phone & email.

Once the user is logged into AuditBoard Site, they can click on the ? icon located in the bottom left corner, then click on 'Contact Support'. Other method is to send an email directly to support@auditboard.com.

Our Customer Support Team is available 24/7/365 to assist with any needs to all of our customers on our platform. They are located in our Headquarters in Southern California. Our guarantee is a reply within 24 business hours.

4.1.4.2. Vendor shall provide a minimum response time of two (2) hours call back for support requests during normal business hours of 8:00 a.m. through 5:00 p.m. Eastern Standard Time Monday through Friday excluding WV state holidays.

Currently our Customer Support Team is available 6AM-6PM PST to assist with any needs to all of our customers on our platform. They are located in our Headquarters in Southern California. Our guarantee is a reply within 24 business hours. A 24 hour answering service is also available for outage and incident reporting.

4.1.5. Cloud-Hosted Saas Professional Services Support

4.1.5.1. Experienced Cloud-hosted Saas consultants, analysts and software developers shall be available to assist WVDOT with software/workflow installation/ configuration/ customizations.

We do not offer professional services. Our training is typically done remotely from our Southern California HQ's by our implementation team. The AuditBoard implementation team will do their best to accommodate different time zones to ensure a successful implementation. We have

teams located in Western, Central, and Eastern parts of the US, in addition to an office located in the UK. Also, our Support Team is based at our HQ's and are available 24/7/365 to assist with any needs to all of our customers domestically and globally.

4.1.5.2. Vendor shall provide both a virtual and on-site rate.
The product is a Cloud based Saas application fully managed by AuditBoard. Deployment to a customer on-prem or virtual environment is not supported.

4.1.5.3. A Statement of Work (SOW) shall be developed that identifies the following:

4.1.5.3.1. Tasks to be performed.

4.1.5.3.2. Deliverables.

4.1.5.3.3. Staff assigned, resumes and experience level.

4.1.5.3.4. Cost breakdown based on the rates bid in this RFQ.

4.1.5.3.5. WVDOT shall review and approve the SOW before commencing of any services

Please refer to our website:
https://www.auditboard.com/implementations/

4.1.6. **Terms and Conditions**

4.1.6.1. Vendor should provide with their bid a copy of any software licensing and or support terms and conditions to which the State of West Virginia or the Agency must agree to or accept, either in writing or digitally, in order to receive the commodities or services offered as part of this contract. Written terms will be required prior to the award of any contract resulting from this soliticaton. Failure to provide additional terms and conditions may result in disqualification or cancellation of the vendor's bid or contract.

4.1.6.2. Please refer to our website for the Subscription Agreement:
https://www.auditboard.com/subscription-agreement/

5. **CONTRACT AWARD:**

   5.1. Contract Award: The Contract is intended to provide the Agency with a purchase price on all Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

   5.2. Pricing Pages: Vendor should complete the Pricing Pages by completing the cost table included as Exhibit A. Vendor should complete the Pricing Pages in their entirety as failure to do so may result in Vendor's bids being disqualified.

   The Pricing Pages contain 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.

   Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation. Confirmed. Our pricing has been filled out in the 'Pricing Pages'.

6. **ORDERING AND PAYMENT:**

   6.1. Ordering: Vendor shall accept orders through wvOASIS, regular mail, facsimile, e-mail, or any other written form of communication. Vendor may, but is not required to, accept on-line orders through a secure internet ordering portal/website. If Vendor has the ability to accept on-line orders, it should include in its response a brief description of how Agencies may utilize the on-line ordering system. Vendor shall ensure that its on-line ordering system is properly secured prior to processing Agency orders on-line. Confirmed.

6.2. Payment: Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

7. DELIVERY AND RETURN:

7.1. Shipment and Delivery: Vendor shall deliver the Contract Items within ten (10) working days after being awarded this Contract and receiving a purchase order or notice to proceed.

7.2. Late Delivery: The Agency placing the order under this Contract must be notified in writing if the shipment of the Contract Items will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the Contract, and/or obtaining the Contract Items from a third party.

Any Agency seeking to obtain the Contract Items from a third party under this provision must first obtain approval of the Purchasing Division.

7.3. Delivery Payment/Risk of Loss: Vendor shall deliver the Contract Items F.O.B. destination to the Agency's location. Vendor shall include the cost of order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery.

7.4. Return of Unacceptable Items: If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return within five (5) days of being notified that item(s) are unacceptable or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

7.5. **Return Due to Agency Error:** Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

8. VENDOR DEFAULT:

8.1. The following shall be considered a vendor default under this Contract.

8.1.1. Failure to provide Contract Items in accordance with the requirements contained herein.

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

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

8.1.4. Failure to remedy deficient performance upon request.

8.2. The following remedies shall be available to Agency upon default.

8.2.1. Immediate cancellation of the Contract.

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

8.2.3. Any other remedies available in law or equity.

9. MISCELLANEOUS:

9.1. No Substitutions: Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

9.2. Vendor Supply: Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

9.3. 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: Tina Yeh

                                                     T

elephone Number: 877.769.5444

Fax Number: 877.769.5444

Email Address: tyeh@auditboard.com

Data Security Policy

1. Overview

Securing data on information assets is a critical step to limiting the loss or exposure of data to unintended parties.

2. Purpose

The objective of this policy is to describe the principles and requirements which must be enforced to secure data stored in or processed in an Information Resource. This policy helps to align AuditBoard procedures with ISO, NIST, and HIPAA requirements.

3. Scope

All information resources containing or processing confidential data and all users of such systems are covered under the scope of this policy.

4. Control Requirements

4.1 Data Storage and Processing Assets

4.1.1 Assets Used for Storage & Transmission of Data

All assets used for the storage and transmission of confidential data must be reviewed by the Information Security team. Assets include network devices, infrastructure environment components, VOIP services, and removable media drives or ports. All devices must support relevant encryption methods and comply with AuditBoard's Access Control Standard.

An assessment of a new infrastructure/environment must be performed by the Information Security team prior to the deployment of the new infrastructure/environment for Confidential data storage or processing.

Only registered removable media should be used to contain AuditBoard data. All un-registered removable media drives/ports must be disabled unless there is a documented and approved business reason for enabling on end-user clients.

4.1.2 Voice & Collaboration Security

Secure solutions are available for audio / video conference calls and collaboration / document sharing platforms where sensitive data is expected to be shared. Secure solutions must be properly authenticated and encrypt data in transit and at rest.

4.2 Encryption & Cryptographic Requirement

4.2.1 Encryption for Data at Rest, In-Transit, and Mobile

Information Resources must employ cryptographic mechanisms to prevent unauthorized disclosure, maintain integrity and communication authenticity of network data traffic over unprotected networks, unless otherwise precluded by law or contract. Appropriate mechanisms (including cryptographic mechanisms) must be used to prevent unauthorized disclosure of Confidential data elements stored at rest. AuditBoard portable media and mobile assets with access to Confidential data must be employed with full disk encryption or file/folder encryption (e.g. EFS, encryption container) when intended to be used/transported/stored outside of an AuditBoard facility.

4.2.2 Approved Cryptographic Solutions

A list of approved cryptographic solutions is maintained by OWASP for [password](#) encryption in transit and [cryptographic](#) storage. Along with an overview of the industry's current "best and approved" libraries for working with encryption. developers should use encryption solutions that follow these practical best practices and seek guidance from security if they have an application which for some reason cannot follow this best practice. The above cryptographic libraries should be used and they must be maintained with up-to-date releases. New cryptographic libraries not on the above lists must be security reviewed or granted exception before adoption within AuditBoard by the Information Security team.

4.2.3 Encryption Key Management Solution Requirements
The defined minimum general requirements must be applied for all AuditBoard implemented and maintained encryption key management. Digital certificates used for authentication must be implemented and configured in a way to ensure security throughout the digital certificates life cycle following the defined requirements listed in the [AuditBoard Cryptographic Standards and Key Management Procedures](#). Securely generated and validated certificates (e.g. digital signature certificates, self-signed certificates, host identifier keys, person identifier keys) must be used and protected following the defined requirements.

4.2.4 Key Custodians and Key Owners (Data Encryption at Rest)
Ownership of Encryption Keys must be assigned to manager level or higher. Authorized AuditBoard employees (contractors or other non-AuditBoard employees are not authorized for this purpose) can be assigned the role of Key Custodian by the Key Owner.

4.3 Data Collection & Verification

4.3.1 Data Collection
The source/provider and the destination/consumer of data (e.g., a system, an application, or a person) must be successfully verified before collecting or generating (e.g. aggregation) any non-public data.

4.3.2 Data Use
Approval for Use of AuditBoard Confidential Data
The requests for using AuditBoard Confidential data for a new purpose (i.e. in a manner different from the original intent / business purpose) must be documented and authorized by the Business Owners, Information Security or AuditBoard Legal as necessary.

4.3.3 Sanitize/Desensitize Sensitive Data Prior to Use
A solution architecture must be designed and deployed to ensure sanitization/de-sensitization of Confidential data prior to being stored or used in other environments, unless there is a documented business reason to retain the Confidential data in its original form.

4.3.4 Data Reproduction Classification
Reproduction of data must be documented, and the risk classification of the original source data must be applied to the reproduced data. Reproduction of non-public data must be authorized by the data owner and with a business need-to-know.

4.4 Technical Controls

4.4.1 Data Loss Prevention Solution
Data Loss Prevention (DLP) solutions must be deployed to monitor for unauthorized transfer of sensitive information. These solutions must be deployed in line with requirements from Legal and the Information Security Team.

4.4.2 Denial of Service Protection
Application or database layer controls must be employed to protect against or limit the effects of denial of service attacks where the availability of the data is critical to the business.

4.4.3 Software, Firmware, And Data-at-Rest Integrity
Integrity verification measures must be applied to detect unauthorized changes to data-at-rest, organization-defined software, firmware and boot applications.

4.4.4 Capability to Support Response to Data Integrity Violation Detection
The information resource, upon detection of a potential data integrity violation, must provide the capability to audit the event and initiate a defined response process that is appropriate to address the incident.

4.4.5 Memory Allocation
Data classified as Confidential must not be in shared memory accessible to unauthorized applications.

4.4.6 Core Dump Disabling
By default, any host that stores or processes AuditBoard Confidential data must be configured to disable memory dumps and exception stack trace logging. This must be documented and known by the data and system owner.

4.4.7 Spoofing Protection:
By default, any host that stores or processes AuditBoard Confidential data must be configured to protect against spoofing with consideration of the following:

- monitoring networks for atypical activity,
- deploying packet filtering to detect inconsistencies (like outgoing packets with source IP addresses that don't match those on the organization's network),
- using robust verification methods (even among networked computers),
- authenticating all IP addresses, and using a network attack blocker.

4.5 Separation of Data & Environments

4.5.1 Separation of Data from Testing to Production
Rules must be defined and documented to enforce separation of data whenever programs/applications are promoted from testing/development to AuditBoard operational or production status.

4.5.2 Separation of Environments
Different environments or types of environments that contain AuditBoard data must be separated with logical controls, in accordance with the Access Control Standard.

5. Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

6. Enforcement

This policy will be enforced by the IT team, department managers, and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

7. Revision Schedule

This policy should be reviewed and updated annually.

8. Management Review History

Policy Details	
Date Written:	3/30/2020
Version:	v3.0
Review Date:	4/2/2023
Approver:	Richard Marcus
Target Audience:	All employees, contractors, consultants, temporary, and other workers at AuditBoard.
Location of Policy:	Guru: https://app.getguru.com/card/Tddj6Byc/Data-Security-Policy AuditBoard: https://auditboard.auditboardapp.com/sh/compliance/policies/71

Version	Reason for Review / Revision Description	Reviewer	Review Date
v1.0	Initial Policy	ISMS Leadership Team	4/28/2020
v1.0	Annual Review	Richard Marcus	3/9/2021
v2.0	Annual Review; Updated Approved	Richard Marcus	4/5/2022

	Cryptographic Solutions, Added Spoofing Protection Control		
V3.0	Annual Review	Richard Marcus	4/2/2023

	Department of Administration **Purchasing Division** **2019 Washington Street East** **Post Office Box 50130** **Charleston, WV 25305-0130**	**State of West Virginia** **Centralized Request for Quote** **Info Technology**

		Reason for Modification:
Proc Folder: 1234689		To attach vendor questions and responses.
Doc Description: Auditing SaaS RFQ (81230134)		Bid opening remains June 28, 2023 at 1:30PM Eastern Time
		No other changes
Proc Type: Central Master Agreement		

Date Issued	Solicitation Closes	Solicitation No	Version
2023-06-16	2023-06-28 13:30	CRFQ 0803 DOT2300000145	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name :   AuditBoard, Inc.

 Address :   12900 Park Plaza Drive Suite 200, Cerritos, CA 90703-9329

 Street :   12900 Park Plaza Drive

City :   Cerritos

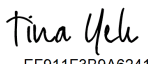**State :**   CA   **Country :**   USA   **Zip :**   90703-9329

Principal Contact :   Sean Mergenthal

Vendor Contact Phone: 856.381.7892   **Extension:**

FOR INFORMATION CONTACT THE BUYER
Larry D McDonnell
304-558-2063
larry.d.mcdonnell@wv.gov

Vendor Signature X *Tina Yeli* ——DocuSigned by:—— EF911F3B9A6241C...   **FEIN#** 47-1299245   **DATE** 6/20/2023

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

ADDITIONAL INFORMATION

REQUEST FOR QUOTATION:

The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Department of Transportation (WVDOT) to establish an open-end contract for auditing cloud-hosted Saas to be utilized by the WV Transportation Division, per the attached documentation.

INVOICE TO	SHIP TO
DEPT. OF TRANSPORTATION	DEPT. OF TRANSPORTATION
1900 KANAWHA BLVD E, BLD. 5 RM-720	1900 KANAWHA BLVD E, BLD. 5 RM-720
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Cloud-based software as a service	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81162000			

Extended Description:
Auditing SaaS RFQ (81230134). See attached pricing page and CRFQ documentation.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Questions due by 4:00 pm EST	2023-06-15

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

AuditBoard Assumption and Exceptions

State of West Virginia, Centralized Request for Quote Info Technology

Use of Customer Contracts: AuditBoard takes exception to customer created terms and conditions and addendums and will negotiate in good faith based on AuditBoard's standard contractual documents. An innovative one-to-many model such as AuditBoard's necessitates a consistent contracting approach with accurate descriptions of what we are delivering and how we deliver it. If selected, AuditBoard will provide a cross-reference as to where provisions are addressed in the AuditBoard contract documents as compared to any sample terms and conditions provided in an RFP. This is the same approach we take with our other large Public Sector customers. We have provided our sample Subscription Agreement for your review.

Since AuditBoard uses our own contractual documents which form the basis of our customer relationships, various traditional RFP concepts such as warranting to requirements, attachment of RFPs or proposals to contracts, etc. don't lend themselves well to the power of one model. AuditBoard's proposals are predicated on use of AuditBoard's standard contractual documents.