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.

Solicitation Response(SR) Dept: 0231 ID: ESR08252600000001348 Ver.: 1 Function: New Phase: Final

Modified by batch , 08/25/2026

Header 3

List View

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

Procurement Folder: 2028979

Procurement Type: Central Master Agreement

Vendor ID: VS0000048590

Legal Name: GovSmart, Inc.

Alias/DBA: GovSmart, Inc.

Total Bid: $696,080.00

Response Date: 08/25/2026

Response Time: 13:20

Responded By User ID: sled@govsmart

First Name: Sarah

Last Name: Lemley

Email: sled@govsmart.com

Phone: 4342842713

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT2700000005

Published Date: 8/18/26

Close Date: 8/25/26

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No 1-Advanced Email Security

Total of Header Attachments: 3

Total of All Attachments: 3

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

State of West Virginia
Solicitation Response

Proc Folder:	2028979
Solicitation Description:	Addendum No 1-Advanced Email Security
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2026-08-25 13:30	SR 0231 ESR08252600000001348	1

VENDOR

VS0000048590
GovSmart, Inc.

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 696080 **Response Date:** 2026-08-25 **Response Time:** 13:20:24

Comments:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@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	Core Detection	22000.000	EA	7.340000	161480.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Core Detection - Year 2 (Optional Renewal)	22000.000	EA	7.710000	169620.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Core Detection - Year 3 (Optional Renewal)	22000.000	EA	8.090000	177980.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Core Detection - Year 4 (Optional Renewal)	22000.000	EA	8.500000	187000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

GovSmart®
Tax ID: 27-1553123 | SAM UEI: DJACUETFQUL8 | CAGE: 5WFZ8
715 Charlton Avenue | Suite 100 | Charlottesville, VA 22903
434.326.5656 | 434.326.5394 Fax | sales@govsmart.com
govsmart.com

Sales Quote

Customer	Ship To	Contract Information		Quote Information	
West Virginia Office of	West Virginia Office of	Type:	OPEN MARKET	**Quote #:**	**GS2026012455**
		Contract #:	OPEN MARKET	Date:	August 18, 2026
		RFQ/RFI #:	20026-21	Expires:	September 30, 2026
		Ship Via:	E-Delivery	Salesperson:	Sarah Lemley
		Lead Time:	E-Delivery	Phone:	434-208-1302
				Email:	sarahlemley@govsmart.com

Line	Manufacturer Part Number	Manufacturer Name	Description	Qty	Unit Price	Extended Price
Base Year						
1	AG04000	Fortra LLC	Cloud Email Protection (12 Months) Fortra, LLC - AG04000	22,000	7.34	161,480.00
2	AG04024	Fortra LLC	Onboarding - CEP Fortra, LLC - AG04024	1	0.00	0
					Base Year Subtotal	161,480.00
Option Year 1						
3	AG04000	Fortra LLC	Cloud Email Protection (12 Months) Fortra, LLC - AG04000	22,000	7.71	169,620.00
4	AG04024	Fortra LLC	Onboarding - CEP Fortra, LLC - AG04024	1	0.00	0
					Option Year 1 Subtotal	169,620.00
Option Year 2						
5	AG04000	Fortra LLC	Cloud Email Protection (12 Months) Fortra, LLC - AG04000	22,000	8.09	177,980.00
6	AG04024	Fortra LLC	Onboarding - CEP Fortra, LLC - AG04024	1	0.00	0
					Option Year 2 Subtotal	177,980.00
Option Year 3						
7	AG04000	Fortra LLC	Cloud Email Protection (12 Months) Fortra, LLC - AG04000	22,000	8.50	187,000.00
8	AG04024	Fortra LLC	Onboarding - CEP Fortra, LLC - AG04024	1	0.00	0
					Option Year 3 Subtotal	187,000.00

GovSmart®

Tax ID: 27-1553123 | SAM UEI: DJACUETFQUL8 | CAGE: 5WFZ8

715 Charlton Avenue | Suite 100 | Charlottesville, VA 22903
434.326.5656 | 434.326.5394 Fax | sales@govsmart.com

govsmart.com

Subtotal	**696,080.00**
Total Tax	0.00
Total $ Incl. Tax	**696,080.00**

GovSmart®
Tax ID: 27-1553123 | SAM UEI: DJACUETFQUL8 | CAGE: 5WFZ8
715 Charlton Avenue | Suite 100 | Charlottesville, VA 22903
434.326.5656 | 434.326.5394 Fax | sales@govsmart.com
govsmart.com

TERMS AND CONDITIONS

GovSmart, Inc. maintains an active SAM.gov registration where all company representations and certifications are readily available, including FAR 52.204-26 Covered Telecommunications Equipment or Services.
Unless otherwise specified within this quote or agreed to by in writing, full payment for order is due within 30 days of invoice date.
Ordering only part of this quote may change the pricing, and a new quote may be required. Contact your sales representative to confirm.
This order may include software subject to a manufacturer's User Agreement or End User License Agreement. Please review the applicable UA or EULA to ensure it is acceptable prior to ordering the software.
Delivery dates on all orders are subject to manufacturer availability. If this is a DPAS-rated order not specified as such on the solicitation, please request delivery notification from your sales representative prior to placing the order.
This quote may include items shipped from different manufacturers or locations that may arrive at different times. In the event of a partial delivery, please provide written authorization, as part of the order, for GovSmart to submit partial invoices for partial deliveries.
Returns: Special/custom built product sales are final and cannot be returned or exchanged. Commercial-off-the-shelf (COTS) items are subject to the manufacturer's standard return policy which can be accessed through the manufacturer's website. Per DODI 5200.48, para. 3.10(b), do not send CUI/FPI to GovSmart using @govsmart.com email addresses. Please contact GovSmart for instructions for securely transmitting CUI/FPI. Invoices not paid within terms are subject to a 1.5% per month interest charge.

For complete terms and conditions for this quote, please visit https://govsmart.com/termsandconditions/

Account: State of West Virginia (000275214)
Base + 3 Option Years
Services terms below include:
Services will be invoiced upon order execution. Services payment is required upfront within Net Terms. Pre-paid services are not dependent on delivery or completion.
Services expire 12 months from the date of purchase. All fees are nonrefundable.
For onsite services, consultant(s) expenses are invoiced following the visit. Customer is responsible for any costs associated with changes in travel arrangements made at the customer's request.
Completion Criteria: Services will end when one of the following first occurs: 1) We complete the project, or 2) We complete the number of hours, or Services expire, or 3) Either of us terminates the project stated with written notice to the other party.
If further assistance is required for services outside of these terms, Fortra will provide another contract for said services.
Scheduled remote working sessions must be scheduled in continuous blocks of time with a minimum of 1-hour blocks for on-demand service requests and 2-hour blocks for implementation and migration services.
The Services shall be performed in accordance with a mutually agreeable schedule. Fortra shall perform the Services during Fortra's normal business hours 8:30am and 5:00pm Monday through Friday at the location of the consultant, excluding holidays, unless otherwise agreed in writing.
If the Services include Fortra installing or updating software on Customers systems, Customer acknowledges that Fortra will not be responsible for any damage to, or disruption of Customers systems or other software. The cumulative liability of Fortra for all claims relating to or from Services will not exceed the total fees paid to Fortra by you.

Any modifications to Fortra products and/or any custom software developed by Fortra for (the "Customized Code") are delivered on an "AS IS" basis without warranty or representation of any kind. Customized Code is not supported by Fortra and is not subject to any maintenance or support plan covering the underlying Fortra products.
The deliverables are delivered to you on an "AS IS" basis without warranty or representation of any kind. Fortra herby disclaims all representations and warranties, express or implied, oral, or written, in fact, arising by operation of law or otherwise, except as expressly stated in this quote and designated as representations or warranties, including without limitation all warranties of merchantability or fitness for a particular purpose. The entire right, title, and interest in and to the Work and the Other Intellectual Property, including without limitation, all copyrights, patent rights, trade secrets and all other worldwide intellectual property rights therein, shall be and remain with Fortra. Any Services work created or developed by Fortra for this engagement are licensed to Customer as part of the underlying Fortra software and are subject to the terms and conditions of the existing license between Fortra and you.
We do our best to accommodate schedule changes, however we require a minimum of 2 business days' notice for scheduled remote working sessions that are less than 8 hours, 5 business days' notice for full-day engagements and 10 business days' notice for changes to scheduled onsite visits. If a cancellation is made within these windows or in the event of a no-show, we reserve the right to charge for the scheduled session/visit.
Services may be terminated by you or Fortra with thirty (30) days written notice if the other party breaches the Services terms unless the breaching party cures the breach within the thirty-day period. Fortra may stop work and terminate Services immediately upon written notice if you fail to make any payment when due to Fortra.
Customer will not solicit or offer employment to any Fortra employee who performs Services under this engagement during the term of this engagement and for a period of six (6) months thereafter. If Customer employs or engages as a consultant an individual who has been assigned by Fortra as a resource for a Services engagement, then Customer shall pay to Fortra a fee of $150,000, as liquidated damages and not as a penalty.

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

Proc Folder: 2028979 **Doc Description:** Addendum No 1-Advanced Email Security **Proc Type:** Central Master Agreement			**Reason for Modification:** Addendum No 1 is issued to publish vendor questions with agency responses and to modify the bid opening date.
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2026-08-18	2026-08-25 13:30	CRFQ 0231 OOT2700000005	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 :

Address :

Street :

City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

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

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

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

ADDITIONAL INFORMATION
Addendum No 1 is issued for the following reasons: 1) To publish vendor questions with the agency's responses. 2) To modify the bid opening date from 8/19/26 to 8/25/26 ---no other changes---

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-08-11

SOLICITATION NUMBER: CRFQ OOT2700000005
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:

Addendum No 1 is issued for the following reasons:

1) To publish vendor questions with the agency's responses.

2) To modify the bid opening date from 8/19/26 to 8/25/26

---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 OOT2700000005

Advanced Email Security

Q.1 : May a single vendor submit more than one quote representing different manufacturer solutions (e.g., two separate bid responses, each featuring a different technology platform)?

Yes. *A single vendor may submit more than one quote as long as each quote independently meets all specifications and is evaluated on its own merits. Each submission must be fully responsive, standalone bid representing one complete solution. The State will evaluate each quote separately and will award to the lowest responsive and responsible bid meeting all requirements, regardless of manufacturer or platform.*

Q.2 Are vendor references or case studies required as part of the bid submission? If so, how many and in what format?

References may be required prior to award, but not mandatory to submit with bids.

Q.3 Inbound threat detection only, or inbound + outbound? IE, Business Email Compromise (BEC) detection User-reported phishing triage/response

The solution must be a complete email security platform that will detect malicious emails in either direction.

Q.4 How does the proposed solution maintain protection and avoid becoming a single point of failure during a Microsoft, Google, or other email platform API outage?

If the email security platform monitors mailboxes via API, it should not become a single point of failure. Mail should still flow even when the API scanning is down. Vendors solution should provide these services.

Q.5 Does WV consider it acceptable for threats to be delivered and remediated after delivery rather than blocked before reaching the recipient or downstream system?

We expect threats to be discovered in near-real-time, within moments of delivery. Messages that are determined to be malicious even several minutes after delivery, should be quarantined.

Q.6 How does the proposed solution prevent zero-click exploits from executing when malicious email content is received, rendered, previewed, or processed, without requiring WV to reroute mail?

The proposed solution should integrate directly with our cloud email provider via API, analyzing and neutralizing hidden payloads at the cloud level in near-real-time or before they can sync to the endpoint. This ensures that zero-click exploits are quarantined before the user's email client ever has a chance to process, render, or preview the malicious content, all without the need to modify MX records or reroute mail.

CRFQ OOT2700000005

Advanced Email Security

Q.7 How does the proposed solution protect collaborative and automated destinations, such as groups, CRM platforms, ticketing systems, and forwarded recipients, without requiring WV to reroute mail?

By connecting directly to our cloud email provider via API, the solution should inspect and neutralize malicious content at the mailbox level before it can be automatically forwarded or ingested by downstream systems like CRMs, ticketing platforms, or group lists. This protects all automated workflows natively from within the cloud environment, completely eliminating the need to alter MX records or reroute mail traffic.

Q.8 How does the proposed solution prevent prompt injection attacks delivered through email without requiring WV to reroute mail?

Using the same direct API integration, the solution should scan incoming emails for malicious instructions, hidden text, and adversarial payloads designed to manipulate AI systems before the content is ever exposed to AI assistants or copilots. This neutralizes prompt injection attacks directly at the cloud inbox layer, keeping downstream AI tools safe without requiring any mail rerouting.

Q.9 Can you provide details on the following dates for this RFQ, after submissions are received?

- Notification of down selection
- Vendor technical demos with the WVOT email security team
- Proof of Concept (POC) start date and preferred trial length
- Date of final contract award
- Implementation kick-off
- Onboarding complete deadline

No dates are available at this time. A post-submission timeline will be developed after bid opening and initial evaluation. All vendors will receive the same schedule once it is finalized. All dates needed by vendor will be posted in Oasis

Q.10 Can we evaluate the ability to learn about your environment based on the 2-4 weeks of POC data rather than adding the prior 90 days of email data?

No. The State will not modify the data requirements outlined in the RFQ. Vendors must provide the prior 90 days of email data as specified. The POC period (2–4 weeks) is intended to validate performance in a live environment, but it does not replace the requirement for historical data.
The State will evaluate both:

- *The vendor's ability to learn from the required 90-day historical dataset, and*
- *The vendor's performance during the POC window.*

Both components are necessary for a complete and responsive evaluation.

CRFQ OOT2700000005

Advanced Email Security

Q.11 Can your organization move forward without this account takeover protection, assuming our solution exceeds expectations in all other categories?

No. Account takeover protection is a required capability under the specifications. The State cannot move forward with a solution that lacks ATO detection, even if the vendor exceeds expectations in other areas. All required capabilities must be met for a bid to be considered responsive. The selected solution should meet all mandatory requirements.

Q.12 Can you please explain the current usage/workflows you have based on the MITRE attack framework?

Our current email security controls are not mapped to the MITRE attack framework.

Q.13 Section 4.1.3.2 requires time-of-click URL inspection. Section 4.1.1.1 prohibits routing mail through any gateway, relay, or proxy, and click-time link rewriting requires modifying the message body before delivery. Would the State confirm whether an API-native approach - extracting and scoring URLs at delivery, continuously re-evaluating them after delivery against updated threat intelligence, and automatically removing a message from all mailboxes when a URL is later determined malicious - satisfies 4.1.3.2, given the non-gateway architecture the solicitation mandates?

The State cannot confirm that the described approach satisfies Section 4.1.3.2. Section 4.1.3.2 requires time-of-click URL inspection, meaning the solution must evaluate URLs at the moment a user clicks them, using real-time analysis.
Section 4.1.1.1 prohibits routing mail through any gateway, relay, or proxy, and prohibits modifying message content (including link rewriting). These architectural constraints remain in effect.
Solutions may use an API-native, non-gateway architecture, but they must still provide true time-of-click inspection as defined in the specifications. Extracting and scoring URLs at delivery, periodically re-evaluating them, and removing messages after delivery does not replace the requirement for real-time, click-moment inspection.
All vendors must meet both the architectural requirements in 4.1.1.1 and the functional requirements in 4.1.3.2 to be considered responsive.

CRFQ OOT2700000005

Advanced Email Security

Q.14 Section 4.1.3.3 requires deep file inspection and cloud-based sandboxing. Would the State clarify whether "sandboxing" requires dynamic detonation of attachments in an isolated execution environment, or whether static structural analysis (macro, embedded-script, archive and container inspection), signature-based scanning, and file-hash threat intelligence together satisfy the requirement?

Section 4.1.3.3 requires deep file inspection and cloud-based sandboxing. For the purposes of this solicitation, sandboxing refers to dynamic detonation of attachments in an isolated execution environment.
Static structural analysis (macro inspection, embedded-script analysis, archive/container inspection), signature-based scanning, and file-hash intelligence are valuable components of a broader detection capability, but they do not replace the requirement for dynamic sandbox detonation as specified in 4.1.3.3.
Solutions may use static analysis in addition to sandboxing, but a solution that relies solely on static methods would not meet the sandboxing requirement.
All vendors must provide both:

- *Deep file inspection, and*
- *Cloud-based sandboxing with dynamic detonation,*

to be considered responsive to Section 4.1.3.3.

Q.15 Definition 3.11 lists JSON, syslog, STIX/TAXII, or API-based delivery as acceptable formats for threat event export. Would the State confirm which formats its SIEM currently ingests, and whether structured JSON event records delivered to State-controlled object storage on a one-minute interval qualify as near-real-time API-based delivery?

Our SentinelOne AI SIEM can ingest data in structured or unstructured data. A one-minute cycle would be acceptable.

Q.16 SaaS Addendum Section 11 requires a CSA STAR Self-Assessment prior to contract award. Would the State clarify whether the questionnaire must accompany the bid or may be submitted after notice of apparent award and prior to execution? Where a prime vendor holds a current CAIQ, does it extend to subcontracted software components?

The CSA STAR Self-Assessment required under SaaS Addendum Section 11 does not need to accompany the bid submission. It must be provided prior to award, if applicable, consistent with the timing of other pre-award security and compliance documents.
Regarding applicability: A prime vendor's existing CSA STAR CAIQ does not automatically extend to subcontracted software components. Each subcontracted component that processes, stores, or transmits State data must be covered by its own CSA STAR Self-Assessment or must be explicitly included within the scope of the prime vendor's assessment. The State will require documentation demonstrating that all components of the proposed solution meet the SaaS Addendum's security and compliance requirements.

CRFQ OOT2700000005

Advanced Email Security

Q.17 SaaS Addendum Section 21 requires compliance with Section 508 accessibility standards. Would the State clarify whether a VPAT or accessibility conformance report must be submitted with the bid, or provided on request following award?

A VPAT or accessibility conformance report is not required at bid submission. Under SaaS Addendum Section 21, the State requires Section 508/WCAG accessibility compliance prior to contract award, which means the VPAT may be submitted after notice of apparent award and before contract execution, along with other pre-award compliance artifacts.
If the State needs additional clarification or documentation during evaluation, it may request it, but it is not a mandatory component of the bid package.
All vendors must ultimately provide a VPAT or equivalent accessibility conformance report covering the entire proposed solution, including any components or modules that process or present content to end users.

Q.18 Section 4.1.2.3 requires retrospective scanning of all existing mailbox contents for the full retention period available within Google Workspace. Would the State confirm the retention period currently configured, the approximate mail volume in scope, and whether "mailbox rules" in this context refers to the current rule state on each mailbox or to the history of rule changes? This refers to the current active state of mailbox rules (e.g., malicious auto-forwarding setups), not a forensic history of rule changes. The current retention period is indefinite, however the retroactive scanning upon implementation may be one year or less. We cannot estimate mail volume.

Section 4.1.2.3 requires retrospective scanning of all existing mailbox contents for the full retention period available within Google Workspace. The State provides the following clarifications:

- *Retention Period: The State's current Google Workspace retention period is indefinite. However, the initial retroactive scanning performed upon implementation may be scoped to approximately one year or less, depending on operational considerations.*
- *Mailbox Rules: In this context, "mailbox rules" refers to the current active state of mailbox rules (e.g., malicious auto-forwarding configurations). It does not refer to a historical or forensic record of rule changes over time.*
- *Mail Volume: The State cannot provide an estimate of total mail volume in scope for retrospective scanning.*

Q.19 Section 4.1.5.1 requires that automated remediation execute without manual administrator approval. Would the State clarify whether fully autonomous action is required at award, or whether remediation executed by a pre-approved SOAR playbook - without a per-message human approval step - satisfies the requirement?

The solution should offer automatic remediation without relying on any external XSOAR

playbooks.

Q.20 The pricing lines reference approximately 22,000 mailboxes. Would the State confirm whether this figure includes shared, delegated, resource, and service-account mailboxes, or reflects licensed human users only?

The estimated 22,000 mailboxes referenced in the pricing lines reflects all potential mailboxes within scope, including licensed user mailboxes as well as shared, delegated, resource, and service-account mailboxes. This figure is provided for pricing purposes to ensure vendors account for the full potential mailbox population that may require protection or scanning under the specifications.

Q.21 Would the State confirm the Google Workspace edition in use, whether all mailboxes reside within a single Workspace tenant, and how many domains are in scope? Would the State also confirm whether Google's own security tooling (for example Security Center and the investigation tool under Enterprise Plus) is currently deployed? Finally, would the State identify the SIEM and SOAR platforms currently in use, and confirm the expected SOAR integration model - specifically, whether the solution should expose an API that the State's SOAR invokes, or accept webhook triggers issued by the SOAR?

The State provides the following clarifications related to Section 4.1.2 and the current Google Workspace environment:

- *Google Workspace Edition & Tenant Structure The State confirms that all mailboxes reside within a single Google Workspace tenant. The specific edition in use will be disclosed after award as part of the onboarding and technical integration process.*
- *Domains in Scope The State will provide the full list of domains after award. Multiple domains exist within the tenant, but the State is not releasing domain counts or names during the solicitation period.*
- *Google Native Security Tooling The State confirms that Google's native security capabilities (e.g., Security Center, Investigation Tool, etc.) are available within the environment. The extent to which these tools are currently deployed or configured will be addressed post-award during technical onboarding.*
- *SIEM and SOAR Platforms The State will identify the specific SIEM and SOAR platforms after award. Vendors should assume integration with a modern enterprise SIEM/SOAR environment capable of consuming standard security event formats.*
- *Expected SOAR Integration Model The State requires that the proposed solution support API-based integration. Solutions may expose an API that the State's SOAR can invoke, and/or accept webhook triggers issued by the State's SOAR. The final integration pattern will be determined collaboratively during implementation.*

All vendors must ensure their proposed solution can support the integration and architectural requirements described in the specifications.

CRFQ OOT2700000005

Advanced Email Security

Q.22 Section 5.0 requires vendors submitting an alternate product to demonstrate compatibility with the State-owned Palo Alto Next-Generation Firewall platform. Would WVTO clarify how this requirement applies to an API-integrated SaaS solution that does not sit in the network data path and does not process network traffic?

Section 5.0 requires vendors submitting an alternate product to demonstrate compatibility with the State-owned Palo Alto Next-Generation Firewall platform. This requirement applies to solutions that interact with or rely on the State's existing Palo Alto security infrastructure.
For an API-integrated SaaS solution that does not sit in the network data path and does not process network traffic, the State clarifies that the requirement is limited to ensuring the proposed solution does not conflict with, interfere with, or require changes to the State's Palo Alto NGFW environment. Because the solution does not route, proxy, or inspect network traffic, traditional NGFW compatibility testing is not applicable.
Vendors submitting an alternate product must still demonstrate that their solution can operate within the State's environment without requiring modifications to the Palo Alto NGFW platform and without introducing architectural conflicts.

Q.23 Would the State consider award of complementary components to more than one vendor - for example an API-integrated inbound detection capability and a separate outbound data-protection capability - or must a single vendor satisfy the entirety of Section 4.1 to be considered responsive?

Section 4.1 defines the required capabilities of the solution. To be considered responsive, a vendor must provide a solution that satisfies all requirements in Section 4.1 within a single, cohesive offering.
The State is not considering a multi-vendor award for complementary components (e.g., one vendor for inbound detection and another for outbound data-protection). Award will be made to the vendor whose single solution meets all mandatory specifications and provides the best overall value to the State.

Q.24 The stated primary objective references "detection and prevention" of phishing and BEC. In a non-gateway, API-integrated architecture, analysis and action occur post-delivery. Would the State clarify whether post-delivery detection combined with automated remediation satisfies the "prevention" objective, or whether "prevention" requires blocking a message before delivery?

The sub-second post-delivery quarantine (detecting and removing the threat via API before the user interacts with it) effectively satisfies the "prevention" requirement.

Q.25 Our solution is hosted in Amazon Web Services (AWS) East/West, with FedRAMP Package ID AGENCYAMAZONEW. Will this suffice for you compliance pathways requirement?

Yes

CRFQ OOT2700000005

Advanced Email Security

Q.26 Would WVOT please define the expectations around tier 3 support (i.e. managed email security, SOC, response, monitoring, incident response, etc.) in further detail?

We require direct access to advanced support team, rather than basic helpdesk support. We expect Tier 3 to assist with complex issues that may arise in the implementation and use of the platform.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT27*005

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.

_____
Company

_____
Authorized Signature

_____
Date

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

	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**

Proc Folder:	2028979	**Reason for Modification:**
Doc Description:	Advanced Email Security	
Proc Type:	Central Master Agreement	

Date Issued	Solicitation Closes	Solicitation No	Version
2026-07-31	2026-08-19 13:30	CRFQ 0231 OOT2700000005	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : GovSmart, Inc.

Address :

Street : 715 Charlton Ave.

City : Charlottesville

State : VA **Country :** USA **Zip :** 22903-5219

Principal Contact : Hamza Durrani

Vendor Contact Phone: 434-326-5656 **Extension:**

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

Vendor Signature X **FEIN#** 27-1553123 **DATE** 8/24/2026

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

ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish an open-end contract for Advanced Email Security layered on top of the Agency's existing Google Workspace environment. The Agency's primary objective is the detection and prevention of phishing attacks, business email compromise (BEC), and related email-based threats that bypass native security controls.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-08-11

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

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

[✔] A pre-bid meeting will not be held prior to bid opening

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

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

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

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

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

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

Submitted emails should have the solicitation number in the subject line. Question

Submission Deadline: Tuesday August 11, 2026 @ 3:00 p.m.

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

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

6. **BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids or modification of bids via email.

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

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

VENDOR NAME:
BUYER: Toby L Welch
SOLICITATION NO.: CRFQ OOT2700000005
BID OPENING DATE: WEDNESDAY AUGUST 19, 2026
BID OPENING TIME: 1:30 P.M.
FAX NUMBER: 304-558-3970

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

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

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

Bid Opening Date and Time: 08/19/26 @ 1:30 P.M.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GENERAL TERMS AND CONDITIONS:

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

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

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

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

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

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

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

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

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

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

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

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

[✓] Term Contract

Initial Contract Term: The Initial Contract Term will be for a period of ONE (1) YEAR. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

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

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

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

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

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

[ ] the contract will continue for _____ years;

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

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

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

[ ] **Other:** Contract Term specified in _____

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

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

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

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

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

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

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

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

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

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

[ ]

[ ]

[ ]

[ ]

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

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

Vendor must maintain:

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

[ ] **Automobile Liability Insurance** in at least an amount of: _____per occurrence.

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

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

[✓] **Cyber Liability Insurance** in an amount of: $2,000,000.00 per occurrence.

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

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

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

[ ]

[ ]

[ ]

[ ]

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

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

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

[ ] _____ for _____.

[ ] Liquidated Damages Contained in the Specifications.

[✓] Liquidated Damages Are Not Included in this Contract.

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

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

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

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

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

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

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

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[✓] Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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) Hamza Durrani, CGO

(Address) 715 Charlton Ave. Charlottesville, VA 22903-5219

(Phone Number) / (Fax Number) 434-326-5656 434-326-5394

(email address) sales@govsmart.com

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

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

GovSmart, Inc.
(Company)

(Signature of Authorized Representative)

Hamza Durrani, CGO
(Printed Name and Title of Authorized Representative) (Date)

434-326-5656 434-326-5394
(Phone Number) (Fax Number)

sales@govsmart.com
(Email Address)

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish an open-end contract for Advanced Email Security layered on top of the Agency's existing Google Workspace environment. The Agency's primary objective is the detection and prevention of phishing attacks, business email compromise (BEC), and related email-based threats that bypass native security controls.

   The State requires a non-gateway, API-integrated architecture that does not modify MX records, does not route email through vendor infrastructure, and operates natively inside Google Workspace.

2. **Current Environment**
   The Agency currently operates Google Workspace including full API access scopes required for security tooling. as its primary email platform across approximately 22,000 mailboxes spanning multiple departments and geographic locations. The Agency seeks a complementary security layer that significantly improves phishing detection rates without disrupting existing email operations. While the current environment is Google Workspace, the proposed solution must be capable of supporting Microsoft 365 natively- *(Natively means that Microsoft 365 support must include API-level access for threat scanning, historical mailbox analysis, automated remediation, mailbox rule monitoring, and time-of-click URL inspection.)* to ensure future flexibility. The Agency also utilizes SIEM/SOAR functions, and any solution deployed must export threat intelligence and event data in formats compatible with the State's existing SIEM/SOAR environment.

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

   3.1 **"Contract Item"** or **"Contract Items"** means the list of items identified in Section 3.1 below and on the Pricing Pages.

   3.2 **"Pricing Pages"** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A, and used to evaluate the Solicitation responses.

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

   3.4 **API-Integrated Deployment"** means a security architecture that connects directly to Google Workspace or Microsoft 365 via vendor-provided APIs without altering MX records, mail routing paths, or introducing intermediary gateways.

   3.5 **Native Support for Microsoft 365"** means full API-level access enabling threat scanning, historical mailbox analysis, automated remediation, mailbox rule monitoring, and URL inspection without requiring mail routing changes.

   3.6 **Historical Scanning"** means retrospective analysis of all existing mailbox contents, including messages, attachments, and mailbox rules, for the full retention period available within Google Workspace or Microsoft 365

   3.7 **Automated Remediation"** means the platform's ability to identify, remove, quarantine, or neutralize malicious emails or artifacts across all mailboxes without manual intervention.

3.8 **US Data Residency"** means all customer data, including email metadata, threat logs, and analysis artifacts, must be stored and processed exclusively within data centers physically located in the United States.

3.9 **Security Information and Event Management (SIEM)"** means the State's centralized security logging and analytics platform that ingests, normalizes, correlates, and retains security-related event data from multiple systems. SIEM platforms are used to detect anomalies, identify threats, and generate alerts based on aggregated log data.

3.10 **Security Orchestration, Automation, and Response (SOAR)"** means the State's automation platform that executes predefined security workflows, playbooks, and remediation actions based on SIEM alerts or external threat events. SOAR platforms enable automated or semi-automated responses such as quarantining emails, disabling accounts, or blocking malicious domains.

3.11 **SIEM/SOAR Compatibility** means the solution must export threat event data in real-time or near-real-time using industry-standard formats (including JSON, syslog, STIX/TAXII, or API-based delivery) and must support automated remediation actions triggered by SOAR playbooks, including global message clawback, mailbox rule removal, and account-level threat response.

3.12 **Mailbox Rule Monitoring** means continuous API-level inspection of mailbox rules, including forwarding, deletion, auto-move, auto-archive, and any rule created or modified by a compromised account.

3.13 **Time-of-Click URL Inspection** means real-time analysis of URLs when a user clicks them, including sandboxing, reputation checks, and detection of morphing or redirected malicious links.

3.14 **Zero Infrastructure Footprint** means the solution requires no on-premises hardware, virtual appliances, local agents, or customer-managed computer resources.

3.15 **Global Message Clawback** means the ability to identify, remove, or quarantine malicious emails across all State mailboxes, regardless of agency, OU, or domain structure, within seconds.

3.16 **Internal-to-Internal Email Traffic** means any email sent between State-managed mailboxes, including cross-agency, cross-domain, and shared mailbox communications, regardless of routing path.

3.17 **Native Workspace Coexistence** means the solution must not disable, degrade, or interfere with Google Workspace or Gemini features, including smart replies, AI-generated summaries, context lookups, and native message rendering.

3.18 **Dual-Platform Flexibility** means the solution must provide full, native API-level functional parity across Google Workspace and Microsoft 365, including historical mailbox scanning, automated remediation, mailbox rule monitoring, time-of-click URL inspection, account-takeover detection, and access to all required Google Workspace and Microsoft Graph API scopes without altering mail routing or requiring gateway-based infrastructure.

3.19 **Inside the perimeter** means operating exclusively through Google Workspace APIs without altering mail routing, MX records, or SMTP paths.

4. GENERAL REQUIREMENTS:

4.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

4.1.1 Core Architectural Requirements (Non-Gateway).

To preserve native email delivery speeds, prevent MX record modifications, and eliminate single-point-of-failure routing risks, the State requires a **native, API-integrated deployment model.**

4.1.1.1.1 **No Gateway Routing:** The solution **must not** require changing the State's MX (Mail Exchanger) records or routing inbound, outbound, or internal email traffic through an external secure email gateway (SEG) appliance, mail relay, or cloud proxy.

4.1.1.1.2 **API-Based Deployment:** The proposed platform must connect directly to the State's Google Workspace environment using Google Workspace APIs.

4.1.1.1.3 **Zero Infrastructure Footprint:** The solution must be 100% cloud-native (SaaS) and require no on-premises hardware, virtual appliances, must not require customer-managed virtual machines or cloud compute resources in any form. or local software installations.

4.1.1.1.4 **Latency-Free Evaluation:** Security analysis must occur asynchronously or inline via API hooks post-delivery, ensuring there is zero artificial latency introduced to standard communication flows.

4.1.1.1.5 **Dual-Platform Flexibility:** While optimized immediately for Google Workspace/Gemini The solution must provide full, native API-level functional parity across Google Workspace and Microsoft 365. Microsoft 365 support must include historical mailbox scanning, automated remediation, mailbox rule monitoring, time-of-click URL inspection, account-takeover detection, and access to all required Microsoft Graph API scopes. The solution must not require MX changes, journaling, SMTP relays, or gateway-based routing for either platform

4.1.2 Gemini & Workspace Functional Integration

The solution must operate exclusively through Google Workspace APIs (inside the perimeter') without altering mail routing or MX records. Internal-to-internal email traffic includes all messages exchanged between State-managed mailboxes across all domains and OUs. The solution must not disable, degrade, or interfere with Gemini features including smart replies, AI-generated summaries, context lookups, or native message rendering. Historical scanning must include all existing mailbox content messages, attachments, and mailbox rules—for the full retention period available within Google Workspace and must begin immediately upon activation.

4.1.2.1 **Internal Threat Detection (East-West Traffic):** Because it sits inside the API tier, the solution must analyze internal-to-internal state emails (employee to employee) for lateral phishing, data exfiltration, or account compromise. Internal-to-internal email traffic includes all messages exchanged between State-managed mailboxes, regardless of domain, OU, or routing path.

4.1.2.2 **Coexistence with Gemini:** The tool must not interfere with Gemini's native capabilities, such as AI-driven draft summaries, smart replies, or workspace context lookups or disable, degrade, or interfere with Gemini features including smart replies, AI-generated summaries, context lookups, and native message rendering.

4.1.2.3 **Historical Scanning:** The API integration must allow the tool to scan existing historical mailboxes retrospectively to establish a baseline threat profile immediately upon activation. Historical scanning must include all existing mailbox contents, including messages, attachments, and mailbox rules, for the full retention period available within Google Workspace. Scanning must begin immediately upon activation and complete without requiring mail routing changes.

4.1.3 Technical & Threat Protection Capabilities

The solution must utilize machine learning that includes behavioral baselining, anomaly detection, and language-pattern analysis beyond static rule-based filtering. BEC detection must include internal and external impersonation, vendor compromise, invoice fraud, and look-alike domain analysis. Time-of-click URL inspection must analyze redirect chains, embedded URLs, QR-encoded links, and dynamically generated phishing pages. Malware and zero-day protection must include deep file inspection and cloud-based sandboxing for executables, archives, scripts, Office documents, PDFs, and containerized payloads. ATO monitoring must include mailbox rule changes, anomalous login behavior, impossible travel detection, OAuth token misuse, MFA bypass attempts, and unauthorized API-scope grants.

4.1.3.1 **Business Email Compromise (BEC) & Spoofing:** Must analyze language sentiment, communication baselines, and look-alike domains to stop executive impersonation, vendor invoice fraud, and employee payroll diversion tactics.

4.1.3.2 **Advanced Phishing & Credential Harvesting:** Must perform real-time URL sandboxing and dynamic link inspection at the time-of-click to block morphing malicious links.

4.1.3.3 **Malware & Zero-Day Attachments:** Must include deep file inspection and sandboxing capabilities for modern vector payloads.

4.1.3.4 **Account Takeover (ATO) Monitoring:** Must monitor mailbox rule modifications (e.g., sneaky auto-forwarding rules created by attackers) and anomalous login behaviors across the state infrastructure.

4.1.4 Compliance, Certifications, & Data Security

4.1.4.1 To maximize vendor competition while ensuring rigorous data security for State infrastructure, the vendor solution must meet **one** of the following compliance pathways. **All customer data must be stored and processed exclusively within the United States**

4.1.4.2 Pathway A — Federal Cloud Alignment (FedRAMP) The vendor must hold a current FedRAMP Authorized (Moderate or High baseline), FedRAMP In-Process, or FedRAMP Ready designation listed on the official FedRAMP Marketplace. FedRAMP Legacy status is not acceptable.

4.1.4.2.1 Vendor should provide the FedRAMP Package ID (PID) for verification.

4.1.4.3 Pathway B (State Cloud Alignment): Hold a current **StateRAMP** Category 2 or 3 Authorization, or maintain a reciprocal, active state-level cloud authorization (e.g., TX-RAMP).

4.1.4.4 Pathway C (Commercial Enterprise Security Framework): Hold a validated **SOC 2 Type II** certification *plus* a signed addendum outlining **Strict Data-Isolation Protocols**. This protocol must explicitly verify:

4.1.4.4.1 State of West Virginia data is logically or physically isolated from other commercial tenants.

4.1.4.4.2 The solution uses end-to-end data encryption both at rest (AES-256) and in transit (TLS 1.3).

4.1.4.4.3 Vendor employees have no zero-trust or un-audited access to mailbox contents.

4.1.4.4.4 Alignment with **NIST SP 800-53** or **ISO/IEC 27001** cybersecurity frameworks.

4.1.5 Administrative & Incident response Automation

4.1.5.1 Automated Remediation (Search & Destroy): When a threat is detected in one mailbox, the tool must have API permissions to automatically find and claw back (quarantine) identical malicious emails across all 22,000 state mailboxes globally in seconds of detection. This must include messages in all domains, agencies, OUs, shared mailboxes, delegated mailboxes, and any mailbox where the malicious message exists. Automated remediation must execute without manual administrator approval and must support SOAR-triggered workflows

4.1.5.2 Role-Based Access Control (RBAC): Must support granular administrative controls allowing specific state department IT staff access to view logs only for their own respective agencies. RBAC must support multi-agency separation, delegated administration, and audit logging of all administrative access.

4.1.6 Vendor Submission Requirements

Vendors responding to this RFQ must explicitly provide answers to the following in their statement of work:

4.1.6.1 Architecture Verification Statement: Provide an architectural narrative or diagram proving that email traffic flows natively into Google Workspace without passing through an intermediary MX-record route or gateway proxy.US data residency: All customer data must be stored and processed within the United States.

4.1.6.2 Compliance Verification: Explicitly state which verification pathway from **Section 4** the platform satisfies, providing supporting documentation (e.g., FedRAMP ID number, StateRAMP dashboard link, or current SOC 2 Type II report).

4.1.6.3 Deployment Timeline: Confirm that onboarding and full-mailbox API verification can be achieved in under 24 hours without disrupting active state communications.

4.1.6.4 Pricing Structure: Provide flat SaaS pricing based on an annual subscription model for approximately **22,000 mailboxes**, inclusive of all updates, tier-3 support, and incident response automation.

5.0 Any vendor submitting an alternate "or equal" product should provide manufacturer data sheets demonstrating full compatibility with the State-owned Palo Alto Next-Generation Firewall platform with their bids and may be required to do so prior to award. These data sheets should be submitted with the bid, and the State may require additional documentation prior to award. Vendors shall assume all costs associated with installation, configuration, and training for any alternate licenses proposed.

6.0 Vendor should provide pricing for Optional Annual Renewal Years 2, 3, and 4. Optional Annual Renewals will be initiated by the State, agreed to by the Vendor, and executed via Change Order.

7.0 CONTRACT AWARD:

7.1 Contract Award: The Contract is intended to provide Agencies 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.

7.2 Pricing Pages: Vendor should complete the Pricing Pages by providing the license cost. 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 electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

8.0 ORDERING AND PAYMENT:

8.1 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.

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

9.0 DELIVERY AND RETURN:

9.1 Delivery Time: Vendor shall deliver standard orders within ten (10) working days after orders are received. Vendor shall deliver emergency orders within five (5) working day(s) after orders are received. Vendor shall ship all orders in accordance with the above schedule and shall not hold orders until a minimum delivery quantity is met.

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

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

9.3 Delivery Payment/Risk of Loss: Standard order delivery shall be F.O.B. destination to the Agency's location. Vendor shall include the cost of standard order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery. The Agency will pay delivery charges on all emergency orders provided that Vendor invoices those delivery costs as a separate charge with the original freight bill attached to the invoice.

9.4 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 items 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.

9.5 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.

10.0 VENDOR DEFAULT:

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

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

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

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

10.1.4 Failure to remedy deficient performance upon request.

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

10.2.1 Immediate cancellation of the Contract.

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

10.2.3 Any other remedies available in law or equity.

11.0 MISCELLANEOUS:

11.1 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.

11.2 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.

11.3 Reports: Vendor shall provide quarterly reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased, and total dollar value of the items purchased. Vendor shall also provide reports, upon request, showing the items purchased during the term of this Contract, the quantity purchased for each of those items, and the total value of purchases for each of those items. Failure to supply such reports may be grounds for cancellation of this Contract.

11.4 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: _____
Telephone Number: _____
Fax Number: _____
Email Address: _____

APPENDIX A:

SOFTWARE AS A SERVICE ADDENDUM

Software as a Service Addendum

1. Definitions:

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

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

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

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

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

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

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

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

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

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

Restricted data means personal data and non-public data.

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

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

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

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

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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: Hamza Durrani

   Email address: sales@govsmart.com

   Phone Number: 434-326-5656