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.

Header 2

List View

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

Procurement Folder: 2028979
Procurement Type: Central Master Agreement
Vendor ID: VS0000020783
Legal Name: PRESIDIO NETWORKED SOLUTIONS LLC
Alias/DBA:
Total Bid: $357,500.00
Response Date: 08/24/2026
Response Time: 15:34
Responded By User ID: gwiederholt
First Name: Glen
Last Name: Wiederholt
Email: gwiederholt@presidio.com
Phone: 7036061346

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: 2
Total of All Attachments: 2

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 ESR08242600000001282	1

VENDOR

VS0000020783
PRESIDIO NETWORKED SOLUTIONS LLC

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 357500 **Response Date:** 2026-08-24 **Response Time:** 15:34:08

Comments:
1. No historical scanning - 4.1.2.3
2. ATO for gmail is prioritized (It DOES exist for M365) - 4.1.3.4
3. No FedRamp cert - 4.1.4.2
4. No STATE RAMP - 4.1.4.3

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	16.250000	357500.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: 1. No historical scanning - 4.1.2.3
2. ATO for gmail is prioritized (It DOES exist for M365) - 4.1.3.4
3. No FedRamp cert - 4.1.4.2
4. No STATE RAMP - 4.1.4.3

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		

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Not bidding renewal at this time

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		

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Not bidding renewal at this time

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		

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Not bidding renewal at this time

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.

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: VS0000020783
Vendor Name : Presidio Networked Solutions LLC
Address : 12100
Street : Sunset Hills Rd., Suite 300
City : Reston
State : VA **Country :** USA **Zip :** 20190
Principal Contact : Glen Wiederholt
Vendor Contact Phone: 571-485-2714 **Extension:** N/A

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

Vendor Signature X Keith Strehman (Aug 24, 2026 13:37:11 EDT) **FEIN#** 58-1167655 **DATE** 8/24/2026

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.

Presidio Networked Solutions LLC
Company

Keith Strohman Keith Strohman (Aug 24, 2026 13:37:11 EDT)
Authorized Signature

08/24/2026
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: VS0000020783

Vendor Name : Presidio Networked Solutions LLC

Address : 12100

Street : Sunset Hills Rd., Suite 300

City : Reston

State : VA **Country :** USA **Zip :** 20190

Principal Contact : Glen Wiederholt

Vendor Contact Phone: 571-485-2714 **Extension:** N/A

FOR INFORMATION CONTACT THE BUYER

Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X Keith Strahman (Aug 24, 2026 13:37:11 EDT) **FEIN#** 58-1167655 **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	$16.25	$357,500.00

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 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
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 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
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