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 3

List View

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

Procurement Folder: 2028979

Procurement Type: Central Master Agreement

Vendor ID: VS0000037600

Legal Name: VPRIME TECH INC

Alias/DBA:

Total Bid: $216,260.00

Response Date: 08/25/2026

Response Time: 12:49

Responded By User ID: Jan Ghalib

First Name: Jan

Last Name: Ghalib

Email: vprime@vprimetech.com

Phone: 833-333-1314

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 ESR08252600000001344	1

VENDOR

VS0000037600
VPRIME TECH INC

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 216260 **Response Date:** 2026-08-25 **Response Time:** 12:49:31

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	9.830000	216260.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Please accept Vprime Tech Inc.'s quote as our final response to this bid.

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:

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:

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:

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.

VPRIMETECH

Federal Tax-ID: 86-1744919 | DUNS: 118787045
Unique Entity ID: GMWNJZBJ7JA6 | CAGE: 8VZQ8
Nizam Alam
nizam.allam@vprimetech.com

vPrime Tech Inc
1400 Broadfield Blvd
Suite 200
Houston, Texas 77084-5162
(833) 333-1314
vprime@vprimetech.com
www.vprimetech.com

West Virginia Office of Technology
Toby L Welch
(304) 558-8802
Toby.L.Welch@wv.gov
BLDG 5, 10TH FLOOR
Charleston, WV USA
CRFQ 0231 OOT2700000005

QUOTE

Quote #	63290963530
Quote Sent Date	08/25/26
Payment Terms	Net 30
Certified	MBE

Item #	Part Number	Description	Qty	Unit Price	Ext. Price
0001	CF-Enterprise	Term - 12 Months Start Date: 10/01/2026 End Date: 09/30/2027	1	$216,109.47	$216,109.47
				Subtotal	**$216,109.47**
				Total	**$216,109.47**

Lead Time:
Purchase Terms:

CLOUDFLARE.

VENDOR RESPONSE TO CENTRALIZED REQUEST FOR QUOTATION (CRFQ)

Advanced Email Security - CRFQ 0231 0072700000005

Point-by-point specification response - Cloudflare Email Security on Google Workspace and Microsoft 365

SOLICITATION
CRFQ 0231 0072700000005 - Advanced Email Security

ISSUING ENTITY
WV Purchasing Division for the WV Office of Technology (WVOT)

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

QUESTIONS DUE
August 11, 2026 (period closed)

BID OPENING / CLOSE
August 25, 2026, 1:30 PM ET (revised by Addendum No. 1)

ADDENDA
Addendum No. 1 - acknowledge receipt

AWARD BASIS
Lowest overall total cost (Sec. 7.1)

PROPOSED SOLUTION
Cloudflare Email Security (part of Cloudflare One)

DEPLOYMENT ARCHITECTURE
Non-gateway, API-based (no MX change, no message modification)

ENVIRONMENT
Google Workspace primary (~22,000 mailboxes); Microsoft 365 supported

SOLUTION PROVIDER
Cloudflare, Inc.

SUBMITTING VENDOR
Cloudflare, Inc. or its authorized reseller (see Certification and Signature page)

ACCOUNT EXECUTIVE
Gary Kott | gkott@cloudflare.com

Executive summary

Cloudflare Email Security is a cloud-native, non-gateway email security service that layers on top of the State's existing Google Workspace environment without changing MX records and without routing mail through Cloudflare for delivery. Mail continues to flow natively through Google; Cloudflare evaluates messages out of band and applies automated remediation through authorized APIs. The same service supports Microsoft 365 natively through the Microsoft Graph API for future flexibility.

This document responds to every specification in Section 4.1 (and related Sections 3.11, 5.0, and 6.0) and incorporates the clarifications published in **Addendum No. 1** (vendor questions and answers; revised bid opening of August 25, 2026). Each item is tagged Compliant, Partially Compliant, Exception, Informational, or Provided, with grounding in Cloudflare product documentation. Where a specification cannot be met exactly as written under a strict non-gateway model (for example, time-of-click URL inspection, which the State confirmed in Addendum No. 1 must occur at the moment of click), we say so plainly rather than overstate. Commercial pricing is submitted on the official wvOASIS Pricing Pages (Exhibit A), and formal compliance documentation (SOC 2 Type II, ISO 27001, and any applicable FedRAMP package) is available from Cloudflare on request.

Solicitation snapshot

SOLICITATION **CRFQ 0231 0072700000005**	CONTRACT TYPE **Central Master Agreement (open-end)**	COMMODITY CODE **43230000**
ADDENDA **No. 1 published (acknowledge receipt)**	BID CLOSE (REVISED) **Aug 25, 2026, 1:30 PM ET**	AWARD BASIS **Lowest overall total cost**
QUANTITY **~22,000 mailboxes (incl. shared/service)**	TERM **Year 1 + optional renewals Yrs 2-4**	SUBMISSION **wvOASIS / signed; no email bids**

Updated per **Addendum No. 1** (vendor Q&A published; bid opening moved from Aug 19 to Aug 25). The vendor question period is closed.

Exceptions and clarifications

Cloudflare submits this response in good faith and states any deviations from the specifications plainly, consistent with the solicitation's exceptions provision. One formal exception and two clarifications apply; all other specifications are addressed as Compliant, Partially Compliant, or Provided in the sections and matrix below.

- **Exception - 4.1.3.2 (time-of-click URL inspection):** Addendum No. 1 (Q.13) confirms the State requires URL inspection at the exact moment a user clicks, while Section 4.1.1.1 requires a non-gateway architecture with no modification of messages. True time-of-click inspection is delivered by rewriting links within the message, which is an inline function that cannot be performed without modifying messages. This response is submitted as a **non-gateway architecture**, consistent with the State's core requirement in Section 4.1.1.1; Cloudflare therefore takes formal exception to the literal time-of-click mechanism in 4.1.3.2. Cloudflare delivers the protective intent of this requirement - preventing users from reaching malicious links - through scan-time URL reputation and link analysis (including redirect chains and look-alike domains) combined with **continuous post-delivery re-evaluation that automatically removes a message if any link is later found to be malicious**, closing the post-delivery weaponization gap that time-of-click is designed to address.
- **Clarification - 4.1.3.3 (attachment sandboxing):** In addition to deep file inspection, cryptographic hashing, and content-type verification, Cloudflare applies machine-learning and threat-intelligence analysis to attachments. Dynamic detonation coverage against the State's specific file-type profile will be validated during the required proof of concept.

- **Clarification - 4.1.3.4 (account takeover) and 4.1.2.3 (historical scanning):** Account-takeover coverage is delivered through Cloudflare CASB and Access as one cohesive Cloudflare One offering from a single vendor, and Google Workspace historical depth (including the 90 days of prior email the State requires) is confirmed and demonstrated during proof-of-concept scoping.

4.1.1 Core Architecture (Non-Gateway)

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.

4.1.1.1.1

No Gateway Routing

Compliant

> Requirement: No change to MX records; no secure email gateway, relay, or proxy inserted into inbound, outbound, or internal mail flow.

CLOUDFLARE RESPONSE

Cloudflare Email Security deploys on Google Workspace in a **post-delivery model that does not change MX records** and does not place a gateway, relay, or proxy in the mail path. Inbound, outbound, and internal mail continue to be delivered natively by Google. Cloudflare receives a copy of messages for analysis through a native Google Workspace content-compliance (journaling) rule and performs any remediation through authorized Google Workspace API scopes. No mail is dependent on Cloudflare for delivery.

Source: Email Security deployment models (reference architecture); API (post-delivery) deployment.

4.1.1.1.2

API-Based Deployment

Partially Compliant

> Requirement: Connect directly to Google Workspace via vendor-provided APIs, without altering MX records or mail routing.

CLOUDFLARE RESPONSE

For **Microsoft 365**, Cloudflare integrates directly through the **Microsoft Graph API** (agentless, no MX change). For **Google Workspace**, Google does not currently expose a full inbound message-scanning API equivalent to Microsoft Graph. Cloudflare therefore ingests messages for analysis using a native Google Workspace compliance (journaling) rule, and performs directory lookups and automated remediation through authorized Google Workspace API scopes (Gmail API, Admin SDK API, and Cloud Identity API) granted to a dedicated service account with domain-wide delegation.

The net result is a **non-gateway integration with no MX change** that uses Google Workspace APIs for identity and remediation, with message ingestion handled by a native Google compliance rule rather than a standalone pull API. We flag this mechanism distinction transparently so the State can evaluate it precisely against the definition in Section 3.4.

Source: Deployment models; Microsoft 365 Graph API setup; Google Workspace journaling + API-scope setup.

4.1.1.1.3

Zero Infrastructure Footprint

Compliant

> Requirement: 100% cloud-delivered SaaS; no on-premises hardware, virtual appliances, endpoint agents, or customer-managed compute.

CLOUDFLARE RESPONSE

Cloudflare Email Security is delivered entirely as SaaS on Cloudflare's global network. There is **no on-premises hardware, no virtual appliance, no endpoint agent, and no customer-managed compute**. Activation is performed by a Google Workspace or Microsoft 365 administrator authorizing the integration from the Cloudflare One dashboard.

Source: Email Security overview; API deployment (agentless).

4.1.1.1.4

Latency-Free Evaluation

Compliant

> Requirement: Asynchronous or inline-via-API evaluation post-delivery, adding zero latency to mail flow.

CLOUDFLARE RESPONSE

Because evaluation is **post-delivery and out of band**, Cloudflare adds **zero latency to mail flow**. Google or Microsoft delivers each message to the user on its normal path while Cloudflare analyzes a copy and applies automated action when a threat is identified. This matches the asynchronous, post-delivery model the State has specified.

Transparency note: Any post-delivery / API architecture (including the one the State specified) has an inherent short dwell time between native delivery and automated remediation. This is a property of the non-gateway model, not added mail-flow latency.

Source: API deployment behavior.

4.1.1.1.5

Dual-Platform Flexibility (Google Workspace + Microsoft 365)

Partially Compliant

> Requirement: Native API-level parity across Google Workspace and Microsoft 365 - historical mailbox analysis, automated remediation, mailbox rule monitoring, time-of-click URL inspection, ATO detection, and Microsoft Graph scopes - with no MX change, journaling, SMTP relay, or gateway.

CLOUDFLARE RESPONSE

Microsoft 365: full native Microsoft Graph API integration supporting historical mailbox analysis, automated remediation / auto-move, mailbox monitoring, and Graph API scopes.

Google Workspace: automated remediation (move to trash, move to junk, admin-recoverable delete), threat detection, and directory integration through authorized Google Workspace API scopes, with message ingestion via a native compliance rule.

Functional coverage is broad on both platforms. In the interest of an honest bid, two mechanism differences are called out: (1) the underlying ingestion differs (M365 Graph API vs Google compliance-rule ingestion plus API remediation), and (2) **time-of-click URL rewriting** is available only in the inline (MX) deployment on either platform, because the non-gateway model does not modify messages (see 4.1.3.2). ATO coverage is addressed in 4.1.3.4.

Source: Deployment models and feature matrix; Auto-move actions (Google + M365).

4.1.2 Gemini and Workspace Functional Integration

Operate via Google Workspace APIs inside the perimeter, without MX changes, and without degrading native Workspace or Gemini functionality.

4.1.2.1

Compliant

Internal Threat Detection (East-West)

> Requirement: Detect internal-to-internal lateral phishing, data exfiltration, and internal account compromise.

CLOUDFLARE RESPONSE

The post-delivery integration can be scoped to inspect **internal-to-internal (east-west) mail**, enabling detection of lateral phishing, internal account compromise, and exfiltration attempts originating from already-trusted internal mailboxes - not just externally inbound mail.

Source: Deployment models (internal message scanning scope).

4.1.2.2

Compliant

Coexistence with Gemini and Native Workspace Features

> Requirement: Must not disable or degrade Gemini smart replies, AI summaries, contextual lookups, or native message rendering.

CLOUDFLARE RESPONSE

Because Cloudflare operates **out of band** (post-delivery, non-gateway) and does not sit in the delivery path or rewrite message bodies in the API / journaling model, it does **not disable or degrade native Google Workspace functionality**, including Gemini smart replies, AI summaries, contextual lookups, and native rendering. Messages are delivered and rendered by Google exactly as they would be without Cloudflare.

Source: API deployment (messages are not modified).

4.1.2.3

Historical Scanning

Partially Compliant

> Requirement: Retrospective analysis of existing mailbox contents (messages, attachments, rules). Addendum No. 1 clarifies (Q.10) that **90 days of prior email must be available for the proof of concept**, and (Q.18) that the initial retroactive scan may be "one year or less," that retention is otherwise indefinite, and that "mailbox rules" means the **current active rule state** (for example, malicious auto-forwarding) rather than a forensic change history.

CLOUDFLARE RESPONSE

Microsoft 365: supported. Cloudflare Retro Scan analyzes existing M365 mail and produces a missed-threat report, and Graph API access enables analysis of existing mailbox contents and current mailbox rules.

Google Workspace: because Google does not expose a full inbound-scanning API, retrospective analysis of pre-existing Google mail is more limited than on M365; the compliance-rule model primarily evaluates mail from activation forward. Cloudflare can inspect the **current active mailbox-rule state** (including risky auto-forwarding) through authorized API scopes. The **90 days of prior email required for the proof of concept and the depth of the Google-side one-year retrospective scan** are demonstrated during the proof of concept, which the State requires as part of evaluation.

Source: Retro Scan (Microsoft 365); Addendum No. 1, Q.10 and Q.18.

4.1.3 Threat Protection

Machine-learning behavioral baselining, anomaly detection, and language-pattern analysis across BEC, phishing, malware, and account takeover.

4.1.3.1

Business Email Compromise and Spoofing

Compliant

> Requirement: Language / sentiment analysis, communication baselining, and look-alike domain detection covering executive impersonation, vendor invoice fraud, and payroll diversion.

CLOUDFLARE RESPONSE

Cloudflare's models assess sender and recipient communication patterns, tone / sentiment, and authentication posture. Documented, directly-relevant capabilities include:

- **Impersonation registry** - protects a managed list of likely-impersonated VIPs / executives (with variant and regular-expression matching and directory sync) to catch **executive impersonation** and BEC.
- **ACH-change-from-free-email detection** - flags payroll and payment-change requests sent from free email domains, directly addressing **payroll diversion and vendor invoice / payment fraud**.
- **Domain-age detection** - flags newly registered and **look-alike domains** with configurable malicious / suspicious thresholds.
- **Spoof disposition** - identifies SPF / DKIM / DMARC failures and Envelope-From vs Header-From mismatches.

Source: Impersonation registry; Additional detections (domain age, ACH change); Dispositions and attributes.

4.1.3.2

Exception

Advanced Phishing and Credential Harvesting

> Requirement: Real-time URL sandboxing and dynamic link inspection at time-of-click, covering redirect chains, embedded URLs, QR-encoded links, and dynamically generated phishing pages. Addendum No. 1 (Q.13) confirms the State requires **true time-of-click inspection at the moment the user clicks** and that a delivery-time-plus-re-evaluation API approach does **not** satisfy this, while the 4.1.1.1 non-gateway and no-message-modification requirements still apply.

CLOUDFLARE RESPONSE

Cloudflare performs strong **URL reputation and link analysis at scan time**, following redirect chains and evaluating destinations (including newly registered and look-alike domains) to drive a malicious disposition and automated removal of messages containing malicious links. This includes continuous post-delivery re-evaluation.

Exception (Addendum No. 1, Q.13): The State requires URL inspection at the exact moment of click, while Section 4.1.1.1 requires a non-gateway architecture with no modification of messages. True time-of-click inspection is delivered by rewriting links within the message so each click is checked in real time, which is an inline function that cannot be performed without modifying messages. Consistent with the non-gateway architecture the State requires in Section 4.1.1.1, Cloudflare takes formal exception to the literal time-of-click mechanism in 4.1.3.2. The protective intent - preventing users from reaching malicious links - is delivered through scan-time URL reputation and link analysis together with **continuous post-delivery re-evaluation and automated removal of any message whose links are later found to be malicious**. See the Exceptions and Clarifications section.

Source: Deployment feature matrix (URL rewriting and link isolation = inline only); API deployment (messages cannot be modified); Addendum No. 1, Q.13 and Q.1.

4.1.3.3

Malware and Zero-Day Attachments

Partially Compliant

> Requirement: Deep file inspection and sandboxing of attachments across executables, archives, scripts, Office documents, PDFs, and containerized payloads, including zero-day payloads. Addendum No. 1 (Q.14) defines "sandboxing" as **dynamic detonation in an isolated execution environment** and states that static, signature, or hash-based analysis alone does **not** satisfy the requirement.

CLOUDFLARE RESPONSE

Attachments across common file classes (executables, archives, scripts, Office documents, and PDFs) are extracted and analyzed. Cloudflare captures cryptographic hashes (MD5, SHA-1, SHA-256, and SSDEEP fuzzy hash) and verifies **declared vs computed content type** (detecting, for example, an executable disguised as an image) and encryption status. Malicious attachments drive a malicious disposition and automated remediation.

Clarification (Addendum No. 1, Q.14): The State defines sandboxing as dynamic detonation in an isolated execution environment. In addition to the deep file inspection, hashing, and content-type verification described above, Cloudflare applies machine-learning and threat-intelligence analysis to attachments. Cloudflare will validate dynamic detonation coverage against the State's specific file-type profile during the required proof of concept.

Source: Email Security Alerts fields (attachment hashing, content-type); Dispositions and attributes; Addendum No. 1, Q.14.

4.1.3.4

Account Takeover (ATO) Monitoring

Partially Compliant

> Requirement: Detect mailbox rule modifications (auto-forward), anomalous logins, impossible travel, OAuth token misuse, MFA bypass, and unauthorized API-scope grants. Addendum No. 1 confirms ATO protection is **mandatory with no waiver** (Q.11) and that the award goes to a **single vendor delivering one cohesive solution** (Q.23).

CLOUDFLARE RESPONSE

Within Email Security: Cloudflare detects email-borne compromise indicators, including lateral / internal phishing sent from a compromised internal mailbox, risky mailbox auto-forwarding rules, and suspicious message behavior.

As one cohesive Cloudflare One offering: the broader ATO signals named here (anomalous logins, impossible travel, OAuth token misuse, MFA-bypass, and unauthorized API-scope grants) are delivered by **Cloudflare CASB** and **Cloudflare Access** within the same Cloudflare One platform and console. To meet the mandatory ATO requirement and the single-vendor condition, Cloudflare bids Email Security together with CASB and Access as **one integrated solution from a single vendor**, not a separable third-party add-on.

Packaging note: Because Q.23 prohibits a multi-vendor award, the ATO components are scoped, licensed, and priced as part of the single Cloudflare One offering, as reflected in the pricing structure (4.1.6.4). CASB and Access sizing is confirmed during scoping.

Source: Cloudflare One (Email Security, CASB, Access); CASB roles in Cloudflare One; Addendum No. 1, Q.11 and Q.23.

4.1.4 Compliance, Certifications, and Data Security

US data residency is required, and the vendor must satisfy at least one compliance pathway (A: FedRAMP, B: StateRAMP / reciprocal, or C: SOC 2 Type II plus a data-isolation addendum).

4.1.4

Compliance Pathway and Data Security

Compliant - Pathway C

> Requirement: Meet Pathway A (FedRAMP), B (StateRAMP / reciprocal such as TX-RAMP), or C (SOC 2 Type II + data isolation: tenant isolation, AES-256 at rest, TLS 1.3 in transit, no un-audited employee mailbox access, aligned to NIST 800-53 or ISO 27001), with all data stored and processed in the United States.

CLOUDFLARE RESPONSE

Cloudflare elects **Pathway C: SOC 2 Type II plus a data-isolation addendum**, and additionally offers supporting attestations:

- **SOC 2 Type II**, **ISO 27001**, ISO 27701, ISO 27018, and PCI DSS - available for download by account Super Administrators through the Cloudflare dashboard and summarized on the Cloudflare Trust Hub.
- **Logical multi-tenant isolation**, **AES-256 encryption at rest**, and **TLS 1.3 in transit** as standard platform controls.
- **US data processing** - Cloudflare Email Security mail processing is performed in the United States, supporting the US Data Residency definition in Section 3.8.

These controls also map to the CRFQ's **Data Security and Privacy Addendum** (post-award obligations): the State retains data ownership, encryption is applied at rest and in transit, Cloudflare supports **multi-factor authentication integration** with the State's identity provider through Cloudflare Access, PCI DSS is available where cardholder data is in scope, and security-incident notification obligations are supported.

FedRAMP / StateRAMP (Pathways A and B): Addendum No. 1 (Q.25) confirms that a valid **FedRAMP Package ID satisfies the compliance pathway**. Cloudflare participates in US public-sector compliance programs and will provide its current authorization status, impact level, and Package ID (PID) applicable to the service on request. Cloudflare's primary pathway for this response is Pathway C (SOC 2 Type II with ISO 27001 and US processing).

Pre-award artifacts (Addendum No. 1): The State also requires a **CSA STAR Self-Assessment (CAIQ)** (Q.16) and a **Section 508 VPAT** covering the whole solution (Q.17) prior to award (not with the bid). Both are tracked in the submission checklist below.

Source: Compliance documentation (SOC 2, ISO, PCI); Cloudflare Trust Hub; Cloudflare Email Security processing region (US).

4.1.5 Administration and Incident Response Automation

4.1.5.1

Automated Remediation (Search and Destroy)

Compliant

> Requirement: Global clawback across all ~22,000 mailboxes (all domains, OUs, shared and delegated mailboxes) without manual approval. Addendum No. 1 (Q.19) clarifies that remediation should be **native and autonomous, not dependent on an external XSOAR playbook**, and (Q.24) that sub-second post-delivery quarantine before the user interacts satisfies the prevention objective.

CLOUDFLARE RESPONSE

Cloudflare **auto-move** policies remediate threats **natively and autonomously** by disposition (malicious, spam, suspicious, spoof, bulk) across all connected mailboxes, domains, and organizational units, **without per-message manual approval and without requiring an external SOAR / XSOAR playbook**. Available actions include move-to-junk, move-to-trash, **admin-recoverable hard delete** (both platforms), and user-recoverable soft delete (Microsoft 365). Remediation is API-driven and centrally policy-controlled, so it applies fleet-wide across all ~22,000 mailboxes. For customers that operate a SOAR, the same actions can **also** be invoked through the Cloudflare API, but this is optional rather than required for remediation to occur.

Wording note: We characterize remediation as automated, near-real-time clawback across the fleet rather than committing to a fixed per-message "seconds" SLA; effective time depends on provider API responsiveness. A specific operational target can be defined during contracting.

Source: Auto-move events; Cloudflare API (SOAR automation).

4.1.5.2

Role-Based Access Control (RBAC)

Compliant

> Requirement: Granular RBAC, per-agency log access, multi-agency separation, delegated administration, and audit logging.

CLOUDFLARE RESPONSE

Cloudflare provides granular, purpose-built Email Security roles:

- **Email Security Analyst** - read and take action on email.
- **Email Security Configuration Admin** - administer settings; cannot read or act on email content.
- **Email Security Integration Admin** - manage integrations only.
- **Email Security Reporting** - metrics only; and **Email Security Read Only**.
- **Cloudflare Zero Trust PII** add-on role - governs who can view personally identifiable data.

Account-scoped roles enable per-agency access separation and delegated administration across a multi-agency tenant, and administrative actions are logged for audit. A read-only mode is also available.

Source: Cloudflare One roles and permissions (Email Security roles); Account-scoped roles.

3.11 SIEM / SOAR Integration

The State operates SIEM / SOAR functions; the solution must export threat intelligence and event data in compatible formats and support SOAR-driven response.

3.11

Threat Data Export and SOAR Response

Compliant

> Requirement: Export in JSON, syslog, STIX / TAXII, or API; support SOAR playbooks (clawback, mailbox-rule removal, account response). Addendum No. 1 (Q.15) identifies the State's SIEM as **SentinelOne AI SIEM**, which ingests structured or unstructured data, and confirms that **JSON delivered to object storage on a one-minute cycle is acceptable** as near-real-time. SOAR integration (Q.21) is API-based (expose an API the SOAR can call and / or accept webhooks).

CLOUDFLARE RESPONSE

Cloudflare **Logpush** provides a dedicated **`email_security_alerts`** dataset in structured **JSON**, including alert IDs, human-readable alert reasons, attachment hashes (MD5 / SHA-1 / SHA-256 / SSDEEP), sender and recipient headers, and dispositions. Logpush delivers on a near-real-time cycle to **S3-compatible object storage** and to common SIEM destinations, and the **Cloudflare API** exposes threat and remediation actions that a SOAR can call. Because SentinelOne AI SIEM ingests JSON directly, **Cloudflare's native JSON output meets this requirement as clarified**; no STIX / TAXII transform is required.

Resolved by Addendum No. 1: The earlier concern that syslog and STIX / TAXII are not native Logpush formats is addressed by Q.15 - the State's SentinelOne SIEM accepts structured JSON to object storage on a one-minute cycle, which Cloudflare Logpush provides natively.

Source: Email Security Alerts (Logpush dataset); Logpush destinations; Cloudflare API.

4.1.6 Vendor Submission Requirements

4.1.6.1

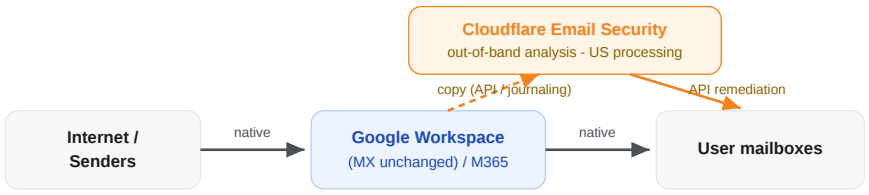
Architecture Verification Statement

Provided

> Requirement: Narrative and diagram proving native mail flow with no MX change and no gateway, and confirming US data residency.

CLOUDFLARE RESPONSE

Statement: Cloudflare Email Security does not change MX records and does not route mail through Cloudflare for delivery. Google Workspace (and, where used, Microsoft 365) delivers mail to users natively. Cloudflare receives an out-of-band copy of messages for analysis and applies remediation through authorized provider APIs. Mail processing is performed in the United States. The diagram below illustrates the flow.



Solid = native mail delivery (unchanged). Dashed orange = out-of-band copy for analysis and API-based remediation.
No MX change. No gateway, relay, or proxy in the delivery path. No customer-managed infrastructure.

Source: Email Security deployment reference architecture.

4.1.6.2

Compliance Verification

Provided

> Requirement: State the selected pathway and provide supporting documentation (FedRAMP PID, StateRAMP link, or SOC 2 report).

CLOUDFLARE RESPONSE

Selected pathway: **Pathway C - SOC 2 Type II plus data-isolation addendum**, supported by ISO 27001 and US data processing (see 4.1.4). The SOC 2 Type II report and ISO / PCI certificates are available to the State under NDA via the Cloudflare dashboard (Super Administrator) and Trust Hub. FedRAMP / StateRAMP authorization status and any applicable Package ID will be provided by Cloudflare on request if the State elects Pathway A or B.

Source: Compliance documentation access; Trust Hub.

4.1.6.3

Deployment Timeline (under 24 hours)

Compliant

> Requirement: Onboarding and full-mailbox API verification achievable in under 24 hours.

CLOUDFLARE RESPONSE

Cloudflare Email Security is designed for rapid, agentless activation. **Microsoft 365** connects through the Graph API in minutes; **Google Workspace** activation (service-account authorization plus the compliance rule) completes well within a single business day. **Full-mailbox API connectivity verification is achievable within 24 hours.**

Caveat: Initial connectivity and protection begin within 24 hours; complete historical / Retro Scan reporting may finish after that connectivity milestone depending on mailbox volume.

Source: Email Security setup; Retro Scan.

4.1.6.4

Pricing Structure

Submitted on Pricing Pages (Exhibit A)

> Requirement: Flat annual SaaS pricing for ~22,000 mailboxes, inclusive of platform updates, tier-3 support, and incident-response automation. Award is on lowest overall total cost across the base year and optional renewal years. Addendum No. 1 clarifies that the ~22,000 count **includes shared, delegated, resource, and service-account mailboxes** (Q.20), and that **Tier 3 support means direct access to an advanced support team** for complex implementation and use issues (Q.26).

CLOUDFLARE RESPONSE

Cloudflare Email Security is licensed as a **flat annual, per-mailbox SaaS subscription**. For this solicitation the subscription is sized to approximately **22,000 mailboxes, counting shared, delegated, resource, and service-account mailboxes** as clarified in Q.20, and is **inclusive of platform updates, advanced (Tier 3) support, and incident-response automation (auto-move / clawback)**. Because the State requires a **single cohesive offering** (Q.23) and mandatory ATO coverage (Q.11), pricing should bundle Email Security with the **Cloudflare One CASB and Access** components that provide ATO. Because award is based on **lowest overall total cost**, all four contract years must be priced on the Pricing Pages. Specific unit pricing, support-tier definition, and any discount schedule are provided by Cloudflare or its authorized reseller on the official Pricing Pages.

LINE	CONTRACT YEAR	QTY (MAILBOXES)	COMMODITY CODE
1	Year 1 (base)	22,000	43230000
2	Year 2 (optional renewal)	22,000	43230000
3	Year 3 (optional renewal)	22,000	43230000
4	Year 4 (optional renewal)	22,000	43230000

Pricing submission: Priced amounts for all four contract years are submitted on the official wvOASIS Pricing Pages (Exhibit A); the line structure above is provided for reference and matches the posted Pricing Pages (unit price governs per the CRFQ). Advanced (Tier 3) support and incident-response automation are included in the subscription.

Additional Solicitation Items

5.0

Palo Alto NGFW Compatibility ("or equal")

Informational

> Requirement: The solicitation references a State-owned Palo Alto Next-Generation Firewall as the baseline for "or equal" evaluation. A vendor offering an alternate must submit **manufacturer data sheets** with the bid to demonstrate compatibility, and the vendor bears any additional installation, configuration, and training costs associated with an alternate.

CLOUDFLARE RESPONSE

Cloudflare Email Security is a cloud-native email security layer and is **complementary to, and does not conflict with, the State's Palo Alto NGFW**. It imposes no dependency on network firewall infrastructure and requires no firewall configuration changes for its non-gateway, API-based operation. The two controls operate at different layers (network perimeter vs. email application) and reinforce one another.

Because Cloudflare Email Security is delivered entirely as SaaS and does not replace or alter the firewall, it adds no installation, configuration, or training cost against the firewall baseline. Where the State requires manufacturer data sheets to evaluate compatibility, Cloudflare product documentation and the architecture statement in 4.1.6.1 support that review; the submission checklist below flags the data-sheet item so it is not missed at bid time.

6.0

Optional Renewal Pricing (Years 2 to 4)

Submitted on Pricing Pages (Exhibit A)

> Requirement: Optional renewal-year pricing for contract Years 2 through 4.

CLOUDFLARE RESPONSE

Renewal pricing for Years 2 through 4 is submitted by Cloudflare or its authorized reseller on the official wvOASIS Pricing Pages (Exhibit A), structured as an annual per-mailbox subscription consistent with Year 1.

Compliance Summary Matrix

At-a-glance status for every specification addressed above.

ITEM	REQUIREMENT	STATUS
4.1.1.1.1	No gateway routing (no MX change)	Compliant
4.1.1.1.2	API-based deployment (Google Workspace)	Partially Compliant
4.1.1.1.3	Zero infrastructure footprint	Compliant
4.1.1.1.4	Latency-free (post-delivery) evaluation	Compliant

ITEM	REQUIREMENT	STATUS
4.1.1.1.5	Dual-platform flexibility (GWS + M365)	Partially Compliant
4.1.2.1	Internal / east-west threat detection	Compliant
4.1.2.2	Coexistence with Gemini / native features	Compliant
4.1.2.3	Historical scanning	Partially Compliant
4.1.3.1	BEC and spoofing	Compliant
4.1.3.2	Advanced phishing / time-of-click URL	Exception
4.1.3.3	Malware and zero-day attachments	Partially Compliant
4.1.3.4	Account takeover (ATO) monitoring	Partially Compliant
4.1.4	Compliance and US data residency	Compliant - Pathway C
4.1.5.1	Automated remediation (search and destroy)	Compliant
4.1.5.2	Role-based access control	Compliant
3.11	SIEM / SOAR export and response	Compliant
4.1.6.1	Architecture verification statement	Provided
4.1.6.2	Compliance verification	Provided
4.1.6.3	Deployment timeline (under 24 hours)	Compliant
4.1.6.4	Pricing structure	Pricing Pages (Exhibit A)
5.0	Palo Alto NGFW ("or equal")	Informational
6.0	Renewal pricing (Years 2 to 4)	Pricing Pages (Exhibit A)

Submission Requirements Checklist

Formal items the CRFQ requires with, or in connection with, the bid. This checklist is a preparation aid; confirm the authoritative list and current versions in wvOASIS before submitting.

- [ ] **Certification and Signature page** - signed by an authorized representative, with FEIN and company details. Unsigned bids are non-responsive.
- [ ] **Completed Pricing Pages (Exhibit A)** - all four contract years (base Year 1 plus optional renewal Years 2 to 4), 22,000 mailboxes per line, commodity code 43230000. Award is on lowest overall total cost; unit price governs.
- [ ] **Addendum Acknowledgement Form** - check the box for **Addendum No. 1** (and any later addenda) and sign the form. Failure to acknowledge addenda can void the bid.
- [ ] **Disclosure of Interested Parties** - WV Code §6D-1-2, submitted before contract work, with a supplemental disclosure within 30 days of any change. Applies to contracts exceeding the statutory threshold.
- [ ] **Data Security and Privacy Addendum (Version 11-1-19)** - reviewed and accepted, including the Appendix A restricted-data designation. Post-award obligations; see 4.1.4.
- [ ] **CSA STAR Self-Assessment (CAIQ)** - required prior to award per SaaS Addendum Sec. 11 (Addendum No. 1, Q.16); any subcontracted components must be covered. Not required with the bid; furnish before award.
- [ ] **Accessibility conformance (VPAT / Section 508 / WCAG)** - required prior to award per SaaS Addendum Sec. 21 (Addendum No. 1, Q.17), covering the full solution including any end-user modules. Not required with the bid; furnish before award.
- [ ] **Palo Alto NGFW manufacturer data sheets** - required only if offering an "or equal" alternate to the referenced firewall. See 5.0. Cloudflare Email Security is complementary SaaS and is not a firewall substitute.
- [ ] **Vendor registration with the WV Purchasing Division** - active registration and the $125 annual fee must be in place before contract award. Registration is not required to submit, but is required to be awarded.
- [ ] **Contract Manager designation** - name a contract manager per Sec. 11.4, and be prepared to provide quarterly and annual usage reports per Sec. 11.3. Post-award administrative requirement.
- [ ] **Exceptions and clarifications** - the formal exception to 4.1.3.2 and related clarifications are stated in the Exceptions and Clarifications section of this response. The vendor question period closed August 11, 2026.
- [ ] **Submission method** - submit through wvOASIS or by signed paper / fax before the August 25, 2026, 1:30 PM ET opening (revised by Addendum No. 1). Email bids are not accepted.

SOURCES REFERENCED

Responses are grounded in Cloudflare product documentation, including: Email Security deployment reference architecture; API (post-delivery) deployment; Microsoft 365 Graph API setup; Retro Scan; Auto-move events; Impersonation registry; Additional detections; Dispositions and attributes; Cloudflare One roles and permissions; the Logpush `email_security_alerts` dataset; and Cloudflare compliance documentation / Trust Hub. Live links are embedded inline throughout this document.

Notes and disclaimer. This technical response maps Cloudflare Email Security capabilities to Solicitation CRFQ 0231 0072700000005 (WVOT Advanced Email Security). Items marked "Partially Compliant" and the formal "Exception" to 4.1.3.2 include a plain-language explanation of the specific limitation and, where applicable, a proposed alternative (for example, true time-of-click URL inspection requires an inline deployment; Google Workspace uses a compliance-rule ingestion model rather than a full pull API; full ATO coverage spans Email Security plus Cloudflare CASB and Access as one Cloudflare One offering). Priced amounts are submitted on the official wvOASIS Pricing Pages (Exhibit A). Compliance reports (SOC 2 Type II, ISO 27001) and any applicable FedRAMP package are available from Cloudflare on request.

Form **W-9**
(Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin. For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See ***Specific Instructions*** on page 3.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

vPrime Tech Inc

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor ☐ C corporation ☑ S corporation ☐ Partnership ☐ Trust/estate

☐ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . .

Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . ☐

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any)

(Applies to accounts maintained outside the United States.)

5 Address (number, street, and apt. or suite no.). See instructions.

1400 Broadfield Boulevard, Suite 200

6 City, state, and ZIP code

Houston, Texas 77084-5162

Requester's name and address (optional)

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

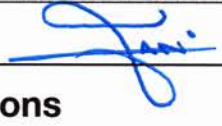
8	6	–	1	7	4	4	9	1	9

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here **Signature of U.S. person**  **Date** 01/05/2026

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

What's New

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

WEST VIRGINIA

STATE TAX DEPARTMENT

BUSINESS REGISTRATION

CERTIFICATE

ISSUED TO:
VPRIME TECH INC
1400 BROADFIELD BLVD 200
HOUSTON, TX 77084-5162

BUSINESS REGISTRATION ACCOUNT NUMBER: **2430-6116**

This certificate is issued on: **07/01/2022**

This certificate is issued by
the West Virginia State Tax Commissioner
in accordance with Chapter 11, Article 12, of the West Virginia Code.

The person or organization identified on this certificate is registered
to conduct business in the State of West Virginia at the location above.

This certificate is not transferrable and must be displayed at the location for which issued.

This certificate shall be permanent until cessation of the business for which the certificate of registration was granted or until it is suspended, revoked or cancelled by the Tax Commissioner.

Change in name or change of location shall be considered a cessation of the business and a new certificate shall be required.

TRAVELING/STREET VENDORS: Must carry a copy of this certificate in every vehicle operated by them.
CONTRACTORS, DRILLING OPERATORS, TIMBER/LOGGING OPERATIONS: Must have a copy of this certificate displayed at every job site within West Virginia.

atL006 v.19
L0473490720

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: Addendum No 1-Advanced Email Security			Addendum No 1 is issued to publish vendor questions with agency responses and to modify the bid opening date.
Proc Type: Central Master Agreement			
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: VS0000037600

Vendor Name : vPrime Tech Inc

Address :

Street : 1400 Broadfield Boulevard Suite 200

City : Houston,

State : TX **Country :** Harris **Zip :** 77084-5162

Principal Contact : Jan Ghalib

Vendor Contact Phone: 833-333-1314 **Extension:** 1

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

jan ghalib

Vendor Signature X

861744919
FEIN#

08/25/26
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		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	$9.60	$211,269.47

Comm Code	Manufacturer	Specification	Model #
43230000	Cloudflare	Term - 12 Months Start Date: 10/01/2026 End Date: 09/30/2027	CF-Enterprise

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

	Document Phase	Document Description	Page 4
OOT2700000005	Final	Addendum No 1-Advanced Email Security	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

VPRIMETECH

Federal Tax-ID: 86-1744919 | DUNS: 118787045
Unique Entity ID: GMWNJZBJ7JA6 | CAGE: 8VZQ8
Nizam Alam
nizam.allam@vprimetech.com

vPrime Tech Inc
1400 Broadfield Blvd
Suite 200
Houston, Texas 77084-5162
(833) 333-1314
vprime@vprimetech.com
www.vprimetech.com

West Virginia Office of Technology
Toby L Welch
(304) 558-8802
Toby.L.Welch@wv.gov
BLDG 5, 10TH FLOOR
Charleston, WV USA
CRFQ 0231 OOT2700000005

QUOTE

Quote #	63290963530
Quote Sent Date	08/25/26
Payment Terms	Net 30
Certified	MBE

Item #	Part Number	Description	Qty	Unit Price	Ext. Price
0001	CF-Enterprise	Term - 12 Months Start Date: 10/01/2026 End Date: 09/30/2027	1	$216,109.47	$216,109.47
				Subtotal	**$216,109.47**
				Total	**$216,109.47**

Lead Time:
Purchase Terms:

CLOUDFLARE.

VENDOR RESPONSE TO CENTRALIZED REQUEST FOR QUOTATION (CRFQ)

Advanced Email Security - CRFQ 0231 0072700000005

Point-by-point specification response - Cloudflare Email Security on Google Workspace and Microsoft 365

SOLICITATION
CRFQ 0231 0072700000005 - Advanced Email Security

ISSUING ENTITY
WV Purchasing Division for the WV Office of Technology (WVOT)

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

QUESTIONS DUE
August 11, 2026 (period closed)

BID OPENING / CLOSE
August 25, 2026, 1:30 PM ET (revised by Addendum No. 1)

ADDENDA
Addendum No. 1 - acknowledge receipt

AWARD BASIS
Lowest overall total cost (Sec. 7.1)

PROPOSED SOLUTION
Cloudflare Email Security (part of Cloudflare One)

DEPLOYMENT ARCHITECTURE
Non-gateway, API-based (no MX change, no message modification)

ENVIRONMENT
Google Workspace primary (~22,000 mailboxes); Microsoft 365 supported

SOLUTION PROVIDER
Cloudflare, Inc.

SUBMITTING VENDOR
Cloudflare, Inc. or its authorized reseller (see Certification and Signature page)

ACCOUNT EXECUTIVE
Gary Kott | gkott@cloudflare.com

Executive summary

Cloudflare Email Security is a cloud-native, non-gateway email security service that layers on top of the State's existing Google Workspace environment without changing MX records and without routing mail through Cloudflare for delivery. Mail continues to flow natively through Google; Cloudflare evaluates messages out of band and applies automated remediation through authorized APIs. The same service supports Microsoft 365 natively through the Microsoft Graph API for future flexibility.

This document responds to every specification in Section 4.1 (and related Sections 3.11, 5.0, and 6.0) and incorporates the clarifications published in **Addendum No. 1** (vendor questions and answers; revised bid opening of August 25, 2026). Each item is tagged Compliant, Partially Compliant, Exception, Informational, or Provided, with grounding in Cloudflare product documentation. Where a specification cannot be met exactly as written under a strict non-gateway model (for example, time-of-click URL inspection, which the State confirmed in Addendum No. 1 must occur at the moment of click), we say so plainly rather than overstate. Commercial pricing is submitted on the official wvOASIS Pricing Pages (Exhibit A), and formal compliance documentation (SOC 2 Type II, ISO 27001, and any applicable FedRAMP package) is available from Cloudflare on request.

Solicitation snapshot

SOLICITATION **CRFQ 0231 0072700000005**	CONTRACT TYPE **Central Master Agreement (open-end)**	COMMODITY CODE **43230000**
ADDENDA **No. 1 published (acknowledge receipt)**	BID CLOSE (REVISED) **Aug 25, 2026, 1:30 PM ET**	AWARD BASIS **Lowest overall total cost**
QUANTITY **~22,000 mailboxes (incl. shared/service)**	TERM **Year 1 + optional renewals Yrs 2-4**	SUBMISSION **wvOASIS / signed; no email bids**

Updated per **Addendum No. 1** (vendor Q&A published; bid opening moved from Aug 19 to Aug 25). The vendor question period is closed.

Exceptions and clarifications

Cloudflare submits this response in good faith and states any deviations from the specifications plainly, consistent with the solicitation's exceptions provision. One formal exception and two clarifications apply; all other specifications are addressed as Compliant, Partially Compliant, or Provided in the sections and matrix below.

- **Exception - 4.1.3.2 (time-of-click URL inspection):** Addendum No. 1 (Q.13) confirms the State requires URL inspection at the exact moment a user clicks, while Section 4.1.1.1 requires a non-gateway architecture with no modification of messages. True time-of-click inspection is delivered by rewriting links within the message, which is an inline function that cannot be performed without modifying messages. This response is submitted as a **non-gateway architecture**, consistent with the State's core requirement in Section 4.1.1.1; Cloudflare therefore takes formal exception to the literal time-of-click mechanism in 4.1.3.2. Cloudflare delivers the protective intent of this requirement - preventing users from reaching malicious links - through scan-time URL reputation and link analysis (including redirect chains and look-alike domains) combined with **continuous post-delivery re-evaluation that automatically removes a message if any link is later found to be malicious**, closing the post-delivery weaponization gap that time-of-click is designed to address.
- **Clarification - 4.1.3.3 (attachment sandboxing):** In addition to deep file inspection, cryptographic hashing, and content-type verification, Cloudflare applies machine-learning and threat-intelligence analysis to attachments. Dynamic detonation coverage against the State's specific file-type profile will be validated during the required proof of concept.

- **Clarification - 4.1.3.4 (account takeover) and 4.1.2.3 (historical scanning):** Account-takeover coverage is delivered through Cloudflare CASB and Access as one cohesive Cloudflare One offering from a single vendor, and Google Workspace historical depth (including the 90 days of prior email the State requires) is confirmed and demonstrated during proof-of-concept scoping.

4.1.1 Core Architecture (Non-Gateway)

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.

4.1.1.1.1

No Gateway Routing

Compliant

> Requirement: No change to MX records; no secure email gateway, relay, or proxy inserted into inbound, outbound, or internal mail flow.

CLOUDFLARE RESPONSE

Cloudflare Email Security deploys on Google Workspace in a **post-delivery model that does not change MX records** and does not place a gateway, relay, or proxy in the mail path. Inbound, outbound, and internal mail continue to be delivered natively by Google. Cloudflare receives a copy of messages for analysis through a native Google Workspace content-compliance (journaling) rule and performs any remediation through authorized Google Workspace API scopes. No mail is dependent on Cloudflare for delivery.

Source: Email Security deployment models (reference architecture); API (post-delivery) deployment.

4.1.1.1.2

API-Based Deployment

Partially Compliant

> Requirement: Connect directly to Google Workspace via vendor-provided APIs, without altering MX records or mail routing.

CLOUDFLARE RESPONSE

For **Microsoft 365**, Cloudflare integrates directly through the **Microsoft Graph API** (agentless, no MX change). For **Google Workspace**, Google does not currently expose a full inbound message-scanning API equivalent to Microsoft Graph. Cloudflare therefore ingests messages for analysis using a native Google Workspace compliance (journaling) rule, and performs directory lookups and automated remediation through authorized Google Workspace API scopes (Gmail API, Admin SDK API, and Cloud Identity API) granted to a dedicated service account with domain-wide delegation.

The net result is a **non-gateway integration with no MX change** that uses Google Workspace APIs for identity and remediation, with message ingestion handled by a native Google compliance rule rather than a standalone pull API. We flag this mechanism distinction transparently so the State can evaluate it precisely against the definition in Section 3.4.

Source: Deployment models; Microsoft 365 Graph API setup; Google Workspace journaling + API-scope setup.

4.1.1.1.3

Zero Infrastructure Footprint

Compliant

> Requirement: 100% cloud-delivered SaaS; no on-premises hardware, virtual appliances, endpoint agents, or customer-managed compute.

CLOUDFLARE RESPONSE

Cloudflare Email Security is delivered entirely as SaaS on Cloudflare's global network. There is **no on-premises hardware, no virtual appliance, no endpoint agent, and no customer-managed compute**. Activation is performed by a Google Workspace or Microsoft 365 administrator authorizing the integration from the Cloudflare One dashboard.

Source: Email Security overview; API deployment (agentless).

4.1.1.1.4

Latency-Free Evaluation

Compliant

> Requirement: Asynchronous or inline-via-API evaluation post-delivery, adding zero latency to mail flow.

CLOUDFLARE RESPONSE

Because evaluation is **post-delivery and out of band**, Cloudflare adds **zero latency to mail flow**. Google or Microsoft delivers each message to the user on its normal path while Cloudflare analyzes a copy and applies automated action when a threat is identified. This matches the asynchronous, post-delivery model the State has specified.

Transparency note: Any post-delivery / API architecture (including the one the State specified) has an inherent short dwell time between native delivery and automated remediation. This is a property of the non-gateway model, not added mail-flow latency.

Source: API deployment behavior.

4.1.1.1.5

Dual-Platform Flexibility (Google Workspace + Microsoft 365)

Partially Compliant

> Requirement: Native API-level parity across Google Workspace and Microsoft 365 - historical mailbox analysis, automated remediation, mailbox rule monitoring, time-of-click URL inspection, ATO detection, and Microsoft Graph scopes - with no MX change, journaling, SMTP relay, or gateway.

CLOUDFLARE RESPONSE

Microsoft 365: full native Microsoft Graph API integration supporting historical mailbox analysis, automated remediation / auto-move, mailbox monitoring, and Graph API scopes.

Google Workspace: automated remediation (move to trash, move to junk, admin-recoverable delete), threat detection, and directory integration through authorized Google Workspace API scopes, with message ingestion via a native compliance rule.

Functional coverage is broad on both platforms. In the interest of an honest bid, two mechanism differences are called out: (1) the underlying ingestion differs (M365 Graph API vs Google compliance-rule ingestion plus API remediation), and (2) **time-of-click URL rewriting** is available only in the inline (MX) deployment on either platform, because the non-gateway model does not modify messages (see 4.1.3.2). ATO coverage is addressed in 4.1.3.4.

Source: Deployment models and feature matrix; Auto-move actions (Google + M365).

4.1.2 Gemini and Workspace Functional Integration

Operate via Google Workspace APIs inside the perimeter, without MX changes, and without degrading native Workspace or Gemini functionality.

4.1.2.1

Compliant

Internal Threat Detection (East-West)

> Requirement: Detect internal-to-internal lateral phishing, data exfiltration, and internal account compromise.

CLOUDFLARE RESPONSE

The post-delivery integration can be scoped to inspect **internal-to-internal (east-west) mail**, enabling detection of lateral phishing, internal account compromise, and exfiltration attempts originating from already-trusted internal mailboxes - not just externally inbound mail.

Source: Deployment models (internal message scanning scope).

4.1.2.2

Compliant

Coexistence with Gemini and Native Workspace Features

> Requirement: Must not disable or degrade Gemini smart replies, AI summaries, contextual lookups, or native message rendering.

CLOUDFLARE RESPONSE

Because Cloudflare operates **out of band** (post-delivery, non-gateway) and does not sit in the delivery path or rewrite message bodies in the API / journaling model, it does **not disable or degrade native Google Workspace functionality**, including Gemini smart replies, AI summaries, contextual lookups, and native rendering. Messages are delivered and rendered by Google exactly as they would be without Cloudflare.

Source: API deployment (messages are not modified).

4.1.2.3

Historical Scanning

Partially Compliant

> Requirement: Retrospective analysis of existing mailbox contents (messages, attachments, rules). Addendum No. 1 clarifies (Q.10) that **90 days of prior email must be available for the proof of concept**, and (Q.18) that the initial retroactive scan may be "one year or less," that retention is otherwise indefinite, and that "mailbox rules" means the **current active rule state** (for example, malicious auto-forwarding) rather than a forensic change history.

CLOUDFLARE RESPONSE

Microsoft 365: supported. Cloudflare Retro Scan analyzes existing M365 mail and produces a missed-threat report, and Graph API access enables analysis of existing mailbox contents and current mailbox rules.

Google Workspace: because Google does not expose a full inbound-scanning API, retrospective analysis of pre-existing Google mail is more limited than on M365; the compliance-rule model primarily evaluates mail from activation forward. Cloudflare can inspect the **current active mailbox-rule state** (including risky auto-forwarding) through authorized API scopes. The **90 days of prior email required for the proof of concept and the depth of the Google-side one-year retrospective scan** are demonstrated during the proof of concept, which the State requires as part of evaluation.

Source: Retro Scan (Microsoft 365); Addendum No. 1, Q.10 and Q.18.

4.1.3 Threat Protection

Machine-learning behavioral baselining, anomaly detection, and language-pattern analysis across BEC, phishing, malware, and account takeover.

4.1.3.1

Business Email Compromise and Spoofing

Compliant

> Requirement: Language / sentiment analysis, communication baselining, and look-alike domain detection covering executive impersonation, vendor invoice fraud, and payroll diversion.

CLOUDFLARE RESPONSE

Cloudflare's models assess sender and recipient communication patterns, tone / sentiment, and authentication posture. Documented, directly-relevant capabilities include:

- **Impersonation registry** - protects a managed list of likely-impersonated VIPs / executives (with variant and regular-expression matching and directory sync) to catch **executive impersonation** and BEC.
- **ACH-change-from-free-email detection** - flags payroll and payment-change requests sent from free email domains, directly addressing **payroll diversion and vendor invoice / payment fraud**.
- **Domain-age detection** - flags newly registered and **look-alike domains** with configurable malicious / suspicious thresholds.
- **Spoof disposition** - identifies SPF / DKIM / DMARC failures and Envelope-From vs Header-From mismatches.

Source: Impersonation registry; Additional detections (domain age, ACH change); Dispositions and attributes.

4.1.3.2

Exception

Advanced Phishing and Credential Harvesting

> Requirement: Real-time URL sandboxing and dynamic link inspection at time-of-click, covering redirect chains, embedded URLs, QR-encoded links, and dynamically generated phishing pages. Addendum No. 1 (Q.13) confirms the State requires **true time-of-click inspection at the moment the user clicks** and that a delivery-time-plus-re-evaluation API approach does **not** satisfy this, while the 4.1.1.1 non-gateway and no-message-modification requirements still apply.

CLOUDFLARE RESPONSE

Cloudflare performs strong **URL reputation and link analysis at scan time**, following redirect chains and evaluating destinations (including newly registered and look-alike domains) to drive a malicious disposition and automated removal of messages containing malicious links. This includes continuous post-delivery re-evaluation.

Exception (Addendum No. 1, Q.13): The State requires URL inspection at the exact moment of click, while Section 4.1.1.1 requires a non-gateway architecture with no modification of messages. True time-of-click inspection is delivered by rewriting links within the message so each click is checked in real time, which is an inline function that cannot be performed without modifying messages. Consistent with the non-gateway architecture the State requires in Section 4.1.1.1, Cloudflare takes formal exception to the literal time-of-click mechanism in 4.1.3.2. The protective intent - preventing users from reaching malicious links - is delivered through scan-time URL reputation and link analysis together with **continuous post-delivery re-evaluation and automated removal of any message whose links are later found to be malicious**. See the Exceptions and Clarifications section.

Source: Deployment feature matrix (URL rewriting and link isolation = inline only); API deployment (messages cannot be modified); Addendum No. 1, Q.13 and Q.1.

4.1.3.3

Malware and Zero-Day Attachments

Partially Compliant

> Requirement: Deep file inspection and sandboxing of attachments across executables, archives, scripts, Office documents, PDFs, and containerized payloads, including zero-day payloads. Addendum No. 1 (Q.14) defines "sandboxing" as **dynamic detonation in an isolated execution environment** and states that static, signature, or hash-based analysis alone does **not** satisfy the requirement.

CLOUDFLARE RESPONSE

Attachments across common file classes (executables, archives, scripts, Office documents, and PDFs) are extracted and analyzed. Cloudflare captures cryptographic hashes (MD5, SHA-1, SHA-256, and SSDEEP fuzzy hash) and verifies **declared vs computed content type** (detecting, for example, an executable disguised as an image) and encryption status. Malicious attachments drive a malicious disposition and automated remediation.

Clarification (Addendum No. 1, Q.14): The State defines sandboxing as dynamic detonation in an isolated execution environment. In addition to the deep file inspection, hashing, and content-type verification described above, Cloudflare applies machine-learning and threat-intelligence analysis to attachments. Cloudflare will validate dynamic detonation coverage against the State's specific file-type profile during the required proof of concept.

Source: Email Security Alerts fields (attachment hashing, content-type); Dispositions and attributes; Addendum No. 1, Q.14.

4.1.3.4

Account Takeover (ATO) Monitoring

Partially Compliant

> Requirement: Detect mailbox rule modifications (auto-forward), anomalous logins, impossible travel, OAuth token misuse, MFA bypass, and unauthorized API-scope grants. Addendum No. 1 confirms ATO protection is **mandatory with no waiver** (Q.11) and that the award goes to a **single vendor delivering one cohesive solution** (Q.23).

CLOUDFLARE RESPONSE

Within Email Security: Cloudflare detects email-borne compromise indicators, including lateral / internal phishing sent from a compromised internal mailbox, risky mailbox auto-forwarding rules, and suspicious message behavior.

As one cohesive Cloudflare One offering: the broader ATO signals named here (anomalous logins, impossible travel, OAuth token misuse, MFA-bypass, and unauthorized API-scope grants) are delivered by **Cloudflare CASB** and **Cloudflare Access** within the same Cloudflare One platform and console. To meet the mandatory ATO requirement and the single-vendor condition, Cloudflare bids Email Security together with CASB and Access as **one integrated solution from a single vendor**, not a separable third-party add-on.

Packaging note: Because Q.23 prohibits a multi-vendor award, the ATO components are scoped, licensed, and priced as part of the single Cloudflare One offering, as reflected in the pricing structure (4.1.6.4). CASB and Access sizing is confirmed during scoping.

Source: Cloudflare One (Email Security, CASB, Access); CASB roles in Cloudflare One; Addendum No. 1, Q.11 and Q.23.

4.1.4 Compliance, Certifications, and Data Security

US data residency is required, and the vendor must satisfy at least one compliance pathway (A: FedRAMP, B: StateRAMP / reciprocal, or C: SOC 2 Type II plus a data-isolation addendum).

4.1.4

Compliance Pathway and Data Security

Compliant - Pathway C

> Requirement: Meet Pathway A (FedRAMP), B (StateRAMP / reciprocal such as TX-RAMP), or C (SOC 2 Type II + data isolation: tenant isolation, AES-256 at rest, TLS 1.3 in transit, no un-audited employee mailbox access, aligned to NIST 800-53 or ISO 27001), with all data stored and processed in the United States.

CLOUDFLARE RESPONSE

Cloudflare elects **Pathway C: SOC 2 Type II plus a data-isolation addendum**, and additionally offers supporting attestations:

- **SOC 2 Type II**, **ISO 27001**, ISO 27701, ISO 27018, and PCI DSS - available for download by account Super Administrators through the Cloudflare dashboard and summarized on the Cloudflare Trust Hub.
- **Logical multi-tenant isolation**, **AES-256 encryption at rest**, and **TLS 1.3 in transit** as standard platform controls.
- **US data processing** - Cloudflare Email Security mail processing is performed in the United States, supporting the US Data Residency definition in Section 3.8.

These controls also map to the CRFQ's **Data Security and Privacy Addendum** (post-award obligations): the State retains data ownership, encryption is applied at rest and in transit, Cloudflare supports **multi-factor authentication integration** with the State's identity provider through Cloudflare Access, PCI DSS is available where cardholder data is in scope, and security-incident notification obligations are supported.

FedRAMP / StateRAMP (Pathways A and B): Addendum No. 1 (Q.25) confirms that a valid **FedRAMP Package ID satisfies the compliance pathway**. Cloudflare participates in US public-sector compliance programs and will provide its current authorization status, impact level, and Package ID (PID) applicable to the service on request. Cloudflare's primary pathway for this response is Pathway C (SOC 2 Type II with ISO 27001 and US processing).

Pre-award artifacts (Addendum No. 1): The State also requires a **CSA STAR Self-Assessment (CAIQ)** (Q.16) and a **Section 508 VPAT** covering the whole solution (Q.17) prior to award (not with the bid). Both are tracked in the submission checklist below.

Source: Compliance documentation (SOC 2, ISO, PCI); Cloudflare Trust Hub; Cloudflare Email Security processing region (US).

4.1.5 Administration and Incident Response Automation

4.1.5.1

Automated Remediation (Search and Destroy)

Compliant

> Requirement: Global clawback across all ~22,000 mailboxes (all domains, OUs, shared and delegated mailboxes) without manual approval. Addendum No. 1 (Q.19) clarifies that remediation should be **native and autonomous, not dependent on an external XSOAR playbook**, and (Q.24) that sub-second post-delivery quarantine before the user interacts satisfies the prevention objective.

CLOUDFLARE RESPONSE

Cloudflare **auto-move** policies remediate threats **natively and autonomously** by disposition (malicious, spam, suspicious, spoof, bulk) across all connected mailboxes, domains, and organizational units, **without per-message manual approval and without requiring an external SOAR / XSOAR playbook**. Available actions include move-to-junk, move-to-trash, **admin-recoverable hard delete** (both platforms), and user-recoverable soft delete (Microsoft 365). Remediation is API-driven and centrally policy-controlled, so it applies fleet-wide across all ~22,000 mailboxes. For customers that operate a SOAR, the same actions can **also** be invoked through the Cloudflare API, but this is optional rather than required for remediation to occur.

Wording note: We characterize remediation as automated, near-real-time clawback across the fleet rather than committing to a fixed per-message "seconds" SLA; effective time depends on provider API responsiveness. A specific operational target can be defined during contracting.

Source: Auto-move events; Cloudflare API (SOAR automation).

4.1.5.2

Role-Based Access Control (RBAC)

Compliant

> Requirement: Granular RBAC, per-agency log access, multi-agency separation, delegated administration, and audit logging.

CLOUDFLARE RESPONSE

Cloudflare provides granular, purpose-built Email Security roles:

- **Email Security Analyst** - read and take action on email.
- **Email Security Configuration Admin** - administer settings; cannot read or act on email content.
- **Email Security Integration Admin** - manage integrations only.
- **Email Security Reporting** - metrics only; and **Email Security Read Only**.
- **Cloudflare Zero Trust PII** add-on role - governs who can view personally identifiable data.

Account-scoped roles enable per-agency access separation and delegated administration across a multi-agency tenant, and administrative actions are logged for audit. A read-only mode is also available.

Source: Cloudflare One roles and permissions (Email Security roles); Account-scoped roles.

3.11 SIEM / SOAR Integration

The State operates SIEM / SOAR functions; the solution must export threat intelligence and event data in compatible formats and support SOAR-driven response.

3.11

Threat Data Export and SOAR Response

Compliant

> Requirement: Export in JSON, syslog, STIX / TAXII, or API; support SOAR playbooks (clawback, mailbox-rule removal, account response). Addendum No. 1 (Q.15) identifies the State's SIEM as **SentinelOne AI SIEM**, which ingests structured or unstructured data, and confirms that **JSON delivered to object storage on a one-minute cycle is acceptable** as near-real-time. SOAR integration (Q.21) is API-based (expose an API the SOAR can call and / or accept webhooks).

CLOUDFLARE RESPONSE

Cloudflare **Logpush** provides a dedicated **`email_security_alerts`** dataset in structured **JSON**, including alert IDs, human-readable alert reasons, attachment hashes (MD5 / SHA-1 / SHA-256 / SSDEEP), sender and recipient headers, and dispositions. Logpush delivers on a near-real-time cycle to **S3-compatible object storage** and to common SIEM destinations, and the **Cloudflare API** exposes threat and remediation actions that a SOAR can call. Because SentinelOne AI SIEM ingests JSON directly, **Cloudflare's native JSON output meets this requirement as clarified**; no STIX / TAXII transform is required.

Resolved by Addendum No. 1: The earlier concern that syslog and STIX / TAXII are not native Logpush formats is addressed by Q.15 - the State's SentinelOne SIEM accepts structured JSON to object storage on a one-minute cycle, which Cloudflare Logpush provides natively.

Source: Email Security Alerts (Logpush dataset); Logpush destinations; Cloudflare API.

4.1.6 Vendor Submission Requirements

4.1.6.1

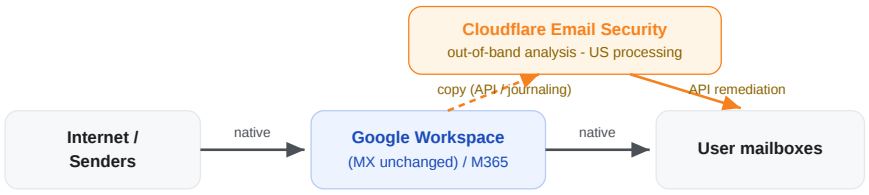
Architecture Verification Statement

Provided

> Requirement: Narrative and diagram proving native mail flow with no MX change and no gateway, and confirming US data residency.

CLOUDFLARE RESPONSE

Statement: Cloudflare Email Security does not change MX records and does not route mail through Cloudflare for delivery. Google Workspace (and, where used, Microsoft 365) delivers mail to users natively. Cloudflare receives an out-of-band copy of messages for analysis and applies remediation through authorized provider APIs. Mail processing is performed in the United States. The diagram below illustrates the flow.



Solid = native mail delivery (unchanged). Dashed orange = out-of-band copy for analysis and API-based remediation.
No MX change. No gateway, relay, or proxy in the delivery path. No customer-managed infrastructure.

Source: Email Security deployment reference architecture.

4.1.6.2

Compliance Verification

Provided

> Requirement: State the selected pathway and provide supporting documentation (FedRAMP PID, StateRAMP link, or SOC 2 report).

CLOUDFLARE RESPONSE

Selected pathway: **Pathway C - SOC 2 Type II plus data-isolation addendum**, supported by ISO 27001 and US data processing (see 4.1.4). The SOC 2 Type II report and ISO / PCI certificates are available to the State under NDA via the Cloudflare dashboard (Super Administrator) and Trust Hub. FedRAMP / StateRAMP authorization status and any applicable Package ID will be provided by Cloudflare on request if the State elects Pathway A or B.

Source: Compliance documentation access; Trust Hub.

4.1.6.3

Deployment Timeline (under 24 hours)

Compliant

> Requirement: Onboarding and full-mailbox API verification achievable in under 24 hours.

CLOUDFLARE RESPONSE

Cloudflare Email Security is designed for rapid, agentless activation. **Microsoft 365** connects through the Graph API in minutes; **Google Workspace** activation (service-account authorization plus the compliance rule) completes well within a single business day. **Full-mailbox API connectivity verification is achievable within 24 hours.**

Caveat: Initial connectivity and protection begin within 24 hours; complete historical / Retro Scan reporting may finish after that connectivity milestone depending on mailbox volume.

Source: Email Security setup; Retro Scan.

4.1.6.4

Pricing Structure

Submitted on Pricing Pages (Exhibit A)

> Requirement: Flat annual SaaS pricing for ~22,000 mailboxes, inclusive of platform updates, tier-3 support, and incident-response automation. Award is on lowest overall total cost across the base year and optional renewal years. Addendum No. 1 clarifies that the ~22,000 count **includes shared, delegated, resource, and service-account mailboxes** (Q.20), and that **Tier 3 support means direct access to an advanced support team** for complex implementation and use issues (Q.26).

CLOUDFLARE RESPONSE

Cloudflare Email Security is licensed as a **flat annual, per-mailbox SaaS subscription**. For this solicitation the subscription is sized to approximately **22,000 mailboxes, counting shared, delegated, resource, and service-account mailboxes** as clarified in Q.20, and is **inclusive of platform updates, advanced (Tier 3) support, and incident-response automation (auto-move / clawback)**. Because the State requires a **single cohesive offering** (Q.23) and mandatory ATO coverage (Q.11), pricing should bundle Email Security with the **Cloudflare One CASB and Access** components that provide ATO. Because award is based on **lowest overall total cost**, all four contract years must be priced on the Pricing Pages. Specific unit pricing, support-tier definition, and any discount schedule are provided by Cloudflare or its authorized reseller on the official Pricing Pages.

LINE	CONTRACT YEAR	QTY (MAILBOXES)	COMMODITY CODE
1	Year 1 (base)	22,000	43230000
2	Year 2 (optional renewal)	22,000	43230000
3	Year 3 (optional renewal)	22,000	43230000
4	Year 4 (optional renewal)	22,000	43230000

Pricing submission: Priced amounts for all four contract years are submitted on the official wvOASIS Pricing Pages (Exhibit A); the line structure above is provided for reference and matches the posted Pricing Pages (unit price governs per the CRFQ). Advanced (Tier 3) support and incident-response automation are included in the subscription.

Additional Solicitation Items

5.0

Palo Alto NGFW Compatibility ("or equal")

Informational

> Requirement: The solicitation references a State-owned Palo Alto Next-Generation Firewall as the baseline for "or equal" evaluation. A vendor offering an alternate must submit **manufacturer data sheets** with the bid to demonstrate compatibility, and the vendor bears any additional installation, configuration, and training costs associated with an alternate.

CLOUDFLARE RESPONSE

Cloudflare Email Security is a cloud-native email security layer and is **complementary to, and does not conflict with, the State's Palo Alto NGFW**. It imposes no dependency on network firewall infrastructure and requires no firewall configuration changes for its non-gateway, API-based operation. The two controls operate at different layers (network perimeter vs. email application) and reinforce one another.

Because Cloudflare Email Security is delivered entirely as SaaS and does not replace or alter the firewall, it adds no installation, configuration, or training cost against the firewall baseline. Where the State requires manufacturer data sheets to evaluate compatibility, Cloudflare product documentation and the architecture statement in 4.1.6.1 support that review; the submission checklist below flags the data-sheet item so it is not missed at bid time.

6.0

Optional Renewal Pricing (Years 2 to 4)

Submitted on Pricing Pages (Exhibit A)

> Requirement: Optional renewal-year pricing for contract Years 2 through 4.

CLOUDFLARE RESPONSE

Renewal pricing for Years 2 through 4 is submitted by Cloudflare or its authorized reseller on the official wvOASIS Pricing Pages (Exhibit A), structured as an annual per-mailbox subscription consistent with Year 1.

Compliance Summary Matrix

At-a-glance status for every specification addressed above.

ITEM	REQUIREMENT	STATUS
4.1.1.1.1	No gateway routing (no MX change)	Compliant
4.1.1.1.2	API-based deployment (Google Workspace)	Partially Compliant
4.1.1.1.3	Zero infrastructure footprint	Compliant
4.1.1.1.4	Latency-free (post-delivery) evaluation	Compliant

ITEM	REQUIREMENT	STATUS
4.1.1.1.5	Dual-platform flexibility (GWS + M365)	Partially Compliant
4.1.2.1	Internal / east-west threat detection	Compliant
4.1.2.2	Coexistence with Gemini / native features	Compliant
4.1.2.3	Historical scanning	Partially Compliant
4.1.3.1	BEC and spoofing	Compliant
4.1.3.2	Advanced phishing / time-of-click URL	Exception
4.1.3.3	Malware and zero-day attachments	Partially Compliant
4.1.3.4	Account takeover (ATO) monitoring	Partially Compliant
4.1.4	Compliance and US data residency	Compliant - Pathway C
4.1.5.1	Automated remediation (search and destroy)	Compliant
4.1.5.2	Role-based access control	Compliant
3.11	SIEM / SOAR export and response	Compliant
4.1.6.1	Architecture verification statement	Provided
4.1.6.2	Compliance verification	Provided
4.1.6.3	Deployment timeline (under 24 hours)	Compliant
4.1.6.4	Pricing structure	Pricing Pages (Exhibit A)
5.0	Palo Alto NGFW ("or equal")	Informational
6.0	Renewal pricing (Years 2 to 4)	Pricing Pages (Exhibit A)

Submission Requirements Checklist

Formal items the CRFQ requires with, or in connection with, the bid. This checklist is a preparation aid; confirm the authoritative list and current versions in wvOASIS before submitting.

- [ ] **Certification and Signature page** - signed by an authorized representative, with FEIN and company details. Unsigned bids are non-responsive.
- [ ] **Completed Pricing Pages (Exhibit A)** - all four contract years (base Year 1 plus optional renewal Years 2 to 4), 22,000 mailboxes per line, commodity code 43230000. Award is on lowest overall total cost; unit price governs.
- [ ] **Addendum Acknowledgement Form** - check the box for **Addendum No. 1** (and any later addenda) and sign the form. Failure to acknowledge addenda can void the bid.
- [ ] **Disclosure of Interested Parties** - WV Code §6D-1-2, submitted before contract work, with a supplemental disclosure within 30 days of any change. Applies to contracts exceeding the statutory threshold.
- [ ] **Data Security and Privacy Addendum (Version 11-1-19)** - reviewed and accepted, including the Appendix A restricted-data designation. Post-award obligations; see 4.1.4.
- [ ] **CSA STAR Self-Assessment (CAIQ)** - required prior to award per SaaS Addendum Sec. 11 (Addendum No. 1, Q.16); any subcontracted components must be covered. Not required with the bid; furnish before award.
- [ ] **Accessibility conformance (VPAT / Section 508 / WCAG)** - required prior to award per SaaS Addendum Sec. 21 (Addendum No. 1, Q.17), covering the full solution including any end-user modules. Not required with the bid; furnish before award.
- [ ] **Palo Alto NGFW manufacturer data sheets** - required only if offering an "or equal" alternate to the referenced firewall. See 5.0. Cloudflare Email Security is complementary SaaS and is not a firewall substitute.
- [ ] **Vendor registration with the WV Purchasing Division** - active registration and the $125 annual fee must be in place before contract award. Registration is not required to submit, but is required to be awarded.
- [ ] **Contract Manager designation** - name a contract manager per Sec. 11.4, and be prepared to provide quarterly and annual usage reports per Sec. 11.3. Post-award administrative requirement.
- [ ] **Exceptions and clarifications** - the formal exception to 4.1.3.2 and related clarifications are stated in the Exceptions and Clarifications section of this response. The vendor question period closed August 11, 2026.
- [ ] **Submission method** - submit through wvOASIS or by signed paper / fax before the August 25, 2026, 1:30 PM ET opening (revised by Addendum No. 1). Email bids are not accepted.

SOURCES REFERENCED

Responses are grounded in Cloudflare product documentation, including: Email Security deployment reference architecture; API (post-delivery) deployment; Microsoft 365 Graph API setup; Retro Scan; Auto-move events; Impersonation registry; Additional detections; Dispositions and attributes; Cloudflare One roles and permissions; the Logpush `email_security_alerts` dataset; and Cloudflare compliance documentation / Trust Hub. Live links are embedded inline throughout this document.

Notes and disclaimer. This technical response maps Cloudflare Email Security capabilities to Solicitation CRFQ 0231 0072700000005 (WVOT Advanced Email Security). Items marked "Partially Compliant" and the formal "Exception" to 4.1.3.2 include a plain-language explanation of the specific limitation and, where applicable, a proposed alternative (for example, true time-of-click URL inspection requires an inline deployment; Google Workspace uses a compliance-rule ingestion model rather than a full pull API; full ATO coverage spans Email Security plus Cloudflare CASB and Access as one Cloudflare One offering). Priced amounts are submitted on the official wvOASIS Pricing Pages (Exhibit A). Compliance reports (SOC 2 Type II, ISO 27001) and any applicable FedRAMP package are available from Cloudflare on request.

Form **W-9**
(Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin. For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See ***Specific Instructions*** on page 3.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

vPrime Tech Inc

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor ☐ C corporation ☑ S corporation ☐ Partnership ☐ Trust/estate

☐ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . .

Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . ☐

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any)

(Applies to accounts maintained outside the United States.)

5 Address (number, street, and apt. or suite no.). See instructions.

1400 Broadfield Boulevard, Suite 200

6 City, state, and ZIP code

Houston, Texas 77084-5162

Requester's name and address (optional)

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

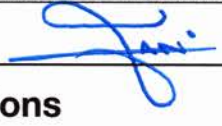
8	6	–	1	7	4	4	9	1	9

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here **Signature of U.S. person**  **Date** 01/05/2026

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

What's New

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

WEST VIRGINIA

STATE TAX DEPARTMENT

BUSINESS REGISTRATION

CERTIFICATE

ISSUED TO:
VPRIME TECH INC
1400 BROADFIELD BLVD 200
HOUSTON, TX 77084-5162

BUSINESS REGISTRATION ACCOUNT NUMBER: **2430-6116**

This certificate is issued on: **07/01/2022**

This certificate is issued by
the West Virginia State Tax Commissioner
in accordance with Chapter 11, Article 12, of the West Virginia Code.

The person or organization identified on this certificate is registered
to conduct business in the State of West Virginia at the location above.

This certificate is not transferrable and must be displayed at the location for which issued.

This certificate shall be permanent until cessation of the business for which the certificate of registration was granted or until it is suspended, revoked or cancelled by the Tax Commissioner.

Change in name or change of location shall be considered a cessation of the business and a new certificate shall be required.

TRAVELING/STREET VENDORS: Must carry a copy of this certificate in every vehicle operated by them.
CONTRACTORS, DRILLING OPERATORS, TIMBER/LOGGING OPERATIONS: Must have a copy of this certificate displayed at every job site within West Virginia.

atL006 v.19
L0473490720

	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: VS0000037600

Vendor Name : vPrime Tech Inc

Address :

Street : 1400 Broadfield Boulevard Suite 200

City : Houston,

State : TX **Country :** Harris **Zip :** 77084-5162

Principal Contact : Jan Ghalib

Vendor Contact Phone: 833-333-1314 **Extension:** 1

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

jan ghalib

Vendor Signature X

861744919

FEIN#

08/25/26

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	$9.60	$211,269.47

Comm Code	Manufacturer	Specification	Model #
43230000	Cloudflare	Term - 12 Months Start Date: 10/01/2026 End Date: 09/30/2027	CF-Enterprise

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.

vPrime Tech Inc

Company

jan ghalib

Authorized Signature

08/25/26

Date

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