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 5

List View

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

Procurement Folder: 2028979
Procurement Type: Central Master Agreement
Vendor ID: VS0000052937
Legal Name: StrongestLayer Inc.
Alias/DBA: StrongestLayer
Total Bid: $726,000.00
Response Date: 08/24/2026
Response Time: 12:24
Responded By User ID: kletain
First Name: Karen
Last Name: Letain
Email: karen@strongestlayer.ai
Phone: 4692887477

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: 5
Total of All Attachments: 5

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 ESR08242600000001270	1

VENDOR

VS0000052937
StrongestLayer Inc.

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 726000 **Response Date:** 2026-08-24 **Response Time:** 12:24:09

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	9.000000	198000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Core Detection - Year 2 (Optional Renewal)	22000.000	EA	8.000000	176000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Core Detection - Year 3 (Optional Renewal)	22000.000	EA	8.000000	176000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Core Detection - Year 4 (Optional Renewal)	22000.000	EA	8.000000	176000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

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

STRONGESTLAYER INC.

Advanced Email Security — Threat Reasoning AI

BID / PROPOSAL RESPONSE

West Virginia Centralized Request for Quotation (CRFQ)

Solicitation No. CRFQ OOT2700000005 — “Advanced Email Security” (OT26077)

Bid Opening: Tuesday, August 25, 2026 at 1:30 p.m. ET

Submitted to:

West Virginia Department of Administration, Purchasing Division
on behalf of the West Virginia Office of Technology (WVOT)
Buyer: Toby L. Welch · 2019 Washington Street East, Charleston, WV 25305-0130
toby.l.welch@wv.gov · (304) 558-8802

Submitted by:

StrongestLayer Inc. · 95 3rd St, 2nd Floor, San Francisco, CA 94103
Primary Contact: Karen Letain, Chief Commercial Officer
karen@strongestlayer.ai · 1-469-288-7477
Date: August 24, 2026

Table of Contents

Section 1: Company Information & Qualifications

1.1 Corporate Information

Company Name: StrongestLayer Inc.
Entity Type: Delaware C-Corporation
Headquarters: 95 3rd St, 2nd Floor, San Francisco, CA 94103
Year Founded: 2024
Domain: strongestlayer.ai
Support Contact: support@strongestlayer.ai

1.2 Officers & Board

Alan LeFort — Chief Executive Officer & Co-Founder

Muhammad Rizwan — Chief Technology Officer & Co-Founder

Joshua Bass — Chief Product Officer & Co-Founder

1.3 Ownership & Investors

StrongestLayer Inc. is a venture-backed company. No entity or individual owns ten percent (10%) or more of the company. Principal investors include Sorenson Capital (lead investor) and Recall Capital.

1.4 Solicitation Contact

Name: Karen Letain
Title: Chief Commercial Officer
Address: 95 3rd St, 2nd Floor, San Francisco, CA 94103
Phone: 1-469-288-7477
Email: karen@strongestlayer.ai

1.5 Registration & Good Standing

StrongestLayer Inc. is registered with the West Virginia Purchasing Division as a vendor in wvOASIS. A Certificate of Good Standing from the Delaware Secretary of State and current SAM.gov registration will be furnished as supplemental documents. The applicable $125 vendor registration fee will be paid prior to contract award.

1.6 Litigation History

StrongestLayer Inc. has not been involved in any litigation during the last five years. The company was incorporated in 2024 and has maintained a clean legal record since its founding.

Section 2: Solution Overview

2.1 The TRACE Platform: Purpose-Built for the AI Era

StrongestLayer's TRACE platform (Threat Reasoning AI Correlation Engine) is built differently from legacy email security tools. While traditional secure email gateways (SEGs) and first-

generation machine-learning bolt-ons rely on pattern matching, known signatures, and historical threat data, TRACE was built from the ground up in 2024 as a multi large language model (LLM)-native security platform. The distinction matters: TRACE does not bolt AI onto older technology — it is AI, built to reason about attacker intent in real time.

Generative AI now lets attackers produce context-rich, grammatically clean phishing emails that bypass traditional detection, because a well-crafted social-engineering message contains no indicators of compromise — no malicious payload, no blacklisted domain, no prior signature. The only way to detect these attacks is to reason about them the way a trained analyst would, at machine speed, across every message. That is what TRACE does for all 22,000 mailboxes in scope for the West Virginia Office of Technology.

2.2 How TRACE Works

TRACE operates via native API integration with both Google Workspace and Microsoft 365. Once authorized by a tenant super administrator (about a fifteen-minute process), the platform analyzes every inbound, outbound, and internal email in real time. There are no MX record changes, no mail-routing modifications, and no impact to existing DMARC, DKIM, or SPF configurations. For each email, TRACE applies multiple large language models to independently evaluate four critical dimensions:

Intent Analysis — What is the sender trying to accomplish? Is the requested action proportional given the relationship between sender and recipient? TRACE catches fraudulent payment, credential, or data requests even when the message carries no malware or link.

Harm Potential — If the recipient complies, what is the financial, operational, or reputational damage? A wire-transfer or vendor-payment-change request to a finance staffer is weighted by the harm it would cause.

Anomaly Detection — Does this email deviate from established communication patterns for this sender, vendor, domain, or internal group? TRACE flags an agency account that suddenly emails dozens of colleagues outside its normal pattern — a sign of a compromised account attacking from the inside.

Deception Markers — Does the email use urgency, authority impersonation, emotional manipulation, or obfuscation to influence behavior? For example, an email impersonating an agency director pressuring staff to act before end of day.

When TRACE determines an email is a threat, it removes or quarantines the message with sub-second response time. TRACE provides explainable verdicts in plain English rather than opaque scores, and classifies each threat against a 44-subtype attack taxonomy — delivering SOC-grade protection without a SOC. Alerts arrive already triaged and explained, so a lean state IT team can verify and act quickly, with high precision and a low false-positive burden.

2.3 Team & Experience

StrongestLayer's leadership team built and ran the last-generation systems that its platform now outperforms. Their careers span the organizations that defined the prior era of email security and threat intelligence — including Proofpoint, FireEye, Mandiant, Google, and McAfee — with more than fifteen years each in building detection and security platforms that leverage adversarial tactics, machine learning, and AI language models. That firsthand understanding of where legacy detection fails allowed us to build a new architecture, designed for the current generation of AI-powered techniques and attacks.

Section 3: Core Architectural Requirements (Spec 4.1.1)

3.1 Architecture Verification Statement (Spec 4.1.6.1)

TRACE is a 100% cloud-native SaaS platform that connects to the State's Google Workspace environment exclusively through Google's published APIs. Email traffic flows natively from the Internet into Google Workspace exactly as it does today: inbound mail resolves against the State's existing MX records and is delivered directly by Google. TRACE never sits in the delivery path. There is no secure email gateway (SEG), no mail relay, no cloud proxy, no journaling, and no SMTP rerouting. Upon delivery, TRACE is notified via API hooks and analyzes each message asynchronously — introducing zero artificial latency to communication flows — and removes or quarantines threats with sub-second target response.

Mail Flow:

```
Internet/Sender → Google Workspace → User Mailbox
                        ↕
                  TRACE (API Tier)
```

Email continues to flow directly into Google Workspace using the customer's existing mail infrastructure. TRACE operates through API-level integration to analyze and protect email without becoming part of the MX routing or mail delivery path.

Because TRACE operates behind the mail-delivery layer rather than inline with it, the platform is fail-open by design: in the event of any StrongestLayer service interruption, email delivery is completely unaffected. This eliminates the single-point-of-failure routing risk the State identifies in Section 4.1.1. The mail-flow illustration above, together with this narrative, constitutes the architecture verification statement required by Spec 4.1.6.1.

3.2 Zero Infrastructure Footprint

TRACE requires no on-premises hardware, no virtual appliances, no customer-managed virtual machines or cloud compute resources, and no software installation on end-user devices. All processing occurs within StrongestLayer's US-based SaaS environment. Existing DMARC, DKIM, and SPF configurations, compliance rules, and routing policies are never altered.

3.3 Dual-Platform Flexibility (Google Workspace & Microsoft 365)

TRACE provides full, native API-level functional parity across Google Workspace and Microsoft 365. Microsoft 365 support operates through Microsoft Graph APIs and includes historical mailbox scanning, automated remediation, mailbox rule monitoring, time-of-click URL inspection, and account-takeover detection — with no MX changes, journaling, SMTP relays, or gateway routing on either platform. Although WVOT operates Google Workspace today, this parity provides the future flexibility required by the specifications.

Section 4: Gemini & Workspace Functional Integration (Spec 4.1.2)

4.1 Internal Threat Detection (East-West Traffic)

Because TRACE sits inside the API tier, it analyzes all internal-to-internal State email — employee to employee, cross-agency, cross-domain, and shared-mailbox traffic, regardless of routing path — for lateral phishing, data exfiltration, and account compromise. This East-West

visibility is essential for catching compromised accounts attacking from inside the perimeter, a capability structurally unavailable to gateway-based products.

4.2 Coexistence with Gemini

TRACE operates exclusively through Google Workspace APIs and does not disable, degrade, or interfere with Gemini or Workspace features, including smart replies, AI-generated summaries, context lookups, and native message rendering.

4.3 Historical Scanning & Baseline Threat Profile

Upon activation, TRACE immediately begins retrospective analysis of existing mailbox contents — messages, attachments, and mailbox rules — for the full retention period available within Google Workspace, without any mail-routing changes. This establishes a baseline threat profile and surfaces pre-existing threats (dormant phishing, malicious rules, prior compromises) from day one. Importantly, TRACE's detection accuracy does not depend on a training window: every message is evaluated on its own content and context, so protection is full-strength immediately while the historical sweep completes in parallel.

Section 5: Technical & Threat Protection Capabilities (Spec 4.1.3)

Machine learning beyond static rules — TRACE applies multiple large language models with behavioral baselining, anomaly detection, and language-pattern analysis to every message — no signatures or static rules required.

BEC & spoofing (4.1.3.1) — Language sentiment, communication-baseline, and look-alike-domain analysis stop executive impersonation, vendor compromise, invoice fraud, and payroll-diversion schemes — including messages that carry no payload or link.

Advanced phishing & credential harvesting (4.1.3.2) — TRACE performs real-time URL analysis on every message at the point of delivery: rather than relying on static reputation lookups, the detection engine actively retrieves and analyzes each URL destination — following full redirect chains, rendering pages in a real browser runtime, and executing client-side JavaScript to expose evasive behavior such as sandbox detection, geofencing, and delayed weaponization. URLs and attachments are never analyzed in isolation: sender history, message intent, and structural indicators carry into every URL verdict, and an unreachable, taken-down, or cloaked destination is itself treated as a detection signal rather than defaulting to a clean verdict. QR-encoded links are extracted via computer vision and analyzed through the same pipeline. TRACE additionally provides time-of-click URL protection: each click on a link in a delivered message is inspected in real time at the moment of user interaction, combining click-time verdict enforcement with the deep destination analysis described above. If a destination has been weaponized after delivery, the click is intercepted and the user is protected before the page loads.

Malware & zero-day attachments (4.1.3.3) — Attachments are dynamically detonated in an isolated cloud sandbox environment, observing actual execution behavior rather than relying on static signatures or file-hash intelligence alone. Deep file inspection covers executables, archives, scripts, Office documents, PDFs, and containerized payloads, including macro and obfuscated-payload analysis, with URLs, attachments, and associated content analyzed together in full message context.

Account takeover monitoring (4.1.3.4) — Supported through TRACE's account-takeover (ATO) signals and suspicious-account-activity analysis, including continuous API-level

monitoring of mailbox rule changes (hidden forwarding, deletion, auto-move rules) and anomalous account behavior. Expanded login-analytics telemetry (impossible-travel detection, OAuth token misuse, MFA bypass attempts) is on StrongestLayer's confirmed ATO roadmap.

Section 6: Compliance, Certifications & Data Security (Spec 4.1.4)

6.1 Compliance Verification Statement (Spec 4.1.6.2)

StrongestLayer satisfies Pathway C — Commercial Enterprise Security Framework. StrongestLayer holds SOC 2 certification (Type II report completed August 2026, available with this bid) and will execute the State's addendum outlining Strict Data-Isolation Protocols, verifying each element of Spec 4.1.4.4:

- State of West Virginia data is logically isolated from all other tenants.
- End-to-end encryption: AES-256 at rest and TLS 1.3 in transit.
- Zero-trust access controls: no un-audited vendor-employee access to mailbox contents; all access is role-based, need-to-know, MFA-protected, and fully logged.
- Security program aligned with NIST SP 800-53 and ISO/IEC 27001 frameworks.

6.2 US Data Residency

All customer data — including email metadata, threat logs, and analysis artifacts — is stored and processed exclusively within data centers physically located in the United States (Amazon Web Services).

6.3 Data Ownership, Retention & Breach Notification

The State retains full ownership of all data. Data is processed solely for threat detection; it is never used for marketing, profiling, or model training for other customers, and never sold or disclosed except as strictly required for threat-detection operations (indicator lookups never include personally identifiable information). Upon termination, data is returned on request and deleted within thirty (30) days with written confirmation, including backups. In the event of a breach involving State data, StrongestLayer provides immediate notification detailing the breach, data affected, remediation, and preventive measures, and cooperates fully with the State's incident-response procedures.

Section 7: Administrative & Incident Response Automation (Spec 4.1.5)

7.1 Automated Remediation — Search & Destroy

When a threat is detected in any mailbox, TRACE automatically identifies and claws back identical and related malicious messages across all 22,000 State mailboxes — all domains, agencies, OUs, shared mailboxes, and delegated mailboxes — within seconds of detection. Remediation executes without manual administrator approval and supports SOAR-triggered workflows. Campaign-sweep analysis finds related variants even when message content has been altered between recipients, and retroactive remediation covers threats weaponized after delivery.

7.2 Role-Based Access Control

TRACE supports granular RBAC with multi-agency separation and delegated administration: agency IT staff can be scoped to view logs and investigations only for their own agency, while WVOT retains central visibility. Distinct read-only/analyst and full-administrator roles are supported, and all administrative access is captured in an audit log with user attribution.

Section 8: SIEM / SOAR & API Integration

Real-time event export — Detection events and log data export in real time or near-real time using industry-standard formats: JSON, syslog, STIX/TAXII, and API-based delivery.

SOAR-triggered actions — SOAR playbooks can trigger automated remediation including global message clawback, mailbox rule removal, and account-level threat response. Detection events can be ingested and managed in Palo Alto Cortex XSOAR, natively or via the StrongestLayer REST API.

REST API — Documented RESTful API for administrative tasks, programmatic data retrieval, and custom alert-management integrations.

Palo Alto NGFW compatibility — Per Addendum No. 1 (Q22), traditional NGFW compatibility testing is not applicable to an API-integrated SaaS solution that does not sit in the network data path and does not process network traffic. StrongestLayer confirms that TRACE operates within the State's environment without requiring any modification to, and without introducing any architectural conflict with, the State-owned Palo Alto NGFW platform.

Section 9: Deployment Timeline (Spec 4.1.6.3)

StrongestLayer confirms that onboarding and full-mailbox API verification are achieved in under 24 hours without disrupting active State communications. Initial API authorization requires approximately 15 minutes with a tenant super administrator; historical scanning and baseline profiling begin immediately upon activation.

StrongestLayer recommends a scoped, phased activation (monitor mode first, then automated remediation upon WVOT approval), with OU-level scoping, weekly check-ins during initial deployment, dashboard training for IT staff at no additional cost, and no end-user training required. All onboarding and training are included in the subscription.

Section 10: Pricing (Spec 4.1.6.4)

10.1 Pricing Structure Statement

StrongestLayer provides flat SaaS pricing on an annual subscription model for approximately 22,000 mailboxes, inclusive of all platform capabilities, all updates, tier-3 support, and incident response automation. There are no implementation fees, no onboarding or training fees, no premium tiers, and no feature gating. Multi-year value is reflected in reduced renewal-year pricing, held firm for the life of the contract.

Contract Item	Est. Qty	Unit Price	Annual Total	
Line 1 — Core Detection per Mailbox, Year 1	22,000	$9.00	$198,000	

Contract Item	Est. Qty	Unit Price	Annual Total	
Line 2 — Year 2 (Optional Renewal)	22,000	$8.00	$176,000	
Line 3 — Year 3 (Optional Renewal)	22,000	$8.00	$176,000	
Line 4 — Year 4 (Optional Renewal)	22,000	$8.00	$176,000	
Total Evaluated Cost (Years 1–4)			**$726,000**	

Unit prices are firm for the life of the contract. Quantities are the State's estimates; actual billing follows actual usage per the Contract. Unit prices prevail in case of any discrepancy.

Section 11: Technical Requirements Response Matrix

The following tables document StrongestLayer's compliance with the mandatory specifications in CRFQ OOT2700000005, Section 4. Response codes: F = Fully Met, P = Partially Met, R = On Roadmap.

A. Core Architectural Requirements (4.1.1)

Requirement	Status	Comments
4.1.1.1.1 No gateway routing / no MX changes	F	API-only architecture; no SEG, relay, proxy, journaling, or MX modification. Fail-open by design.
4.1.1.1.2 API-based deployment (Google Workspace APIs)	F	Direct connection via Google's published APIs; ~15-minute tenant authorization.
4.1.1.1.3 Zero infrastructure footprint	F	100% cloud-native SaaS; no hardware, appliances, VMs, customer compute, or local software.
4.1.1.1.4 Latency-free evaluation	F	Asynchronous post-delivery analysis via API hooks; zero artificial latency; sub-second remediation target.
4.1.1.1.5 Dual-platform flexibility (Google + M365 parity)	F	Full native parity via Microsoft Graph APIs: historical scanning, remediation, rule monitoring, time-of-click inspection, ATO detection. No routing changes on either platform.

B. Gemini & Workspace Functional Integration (4.1.2)

Requirement	Status	Comments
4.1.2.1 Internal threat detection (East-West)	F	All internal-to-internal traffic analyzed across domains, OUs, and shared mailboxes for lateral phishing, exfiltration, and compromise.

Requirement	Status	Comments
4.1.2.2 Coexistence with Gemini	F	No interference with Gemini smart replies, AI summaries, context lookups, or native rendering; message content and rendering untouched.
4.1.2.3 Historical scanning & baseline	F	Immediate retrospective scan of messages, attachments, and mailbox rules for the full Workspace retention period; detection is full-strength from day one — no training window required.

C. Technical & Threat Protection (4.1.3)

Requirement	Status	Comments
ML with behavioral baselining, anomaly detection, language-pattern analysis	F	Multiple LLMs reason over every message; behavioral, anomaly, and language-pattern analysis beyond any static rules.
4.1.3.1 BEC & spoofing	F	Sentiment, communication-baseline, and look-alike-domain analysis; internal and external impersonation, vendor compromise, invoice fraud, payroll diversion.
4.1.3.2 Advanced phishing & credential harvesting (time-of-click)	F	Real-time destination analysis at delivery (browser-runtime rendering, JS execution, full redirect chains, QR via computer vision) plus time-of-click inspection with click-time verdict enforcement; destinations weaponized after delivery are intercepted before page load.
4.1.3.3 Malware & zero-day attachments	F	Dynamic detonation of attachments in an isolated cloud sandbox plus deep file inspection across executables, archives, scripts, Office docs, PDFs, and containerized payloads.
4.1.3.4 Account takeover monitoring	F	ATO signals and suspicious-account-activity analysis, incl. mailbox rule-change monitoring and anomalous account behavior. Expanded login analytics (impossible travel, OAuth misuse, MFA bypass): confirmed ATO roadmap.

D. Compliance, Certifications & Data Security (4.1.4)

Requirement	Status	Comments
4.1.4.1 US data residency	F	All data stored and processed exclusively in US data centers (AWS).
4.1.4.4 Pathway C — Commercial Enterprise Security Framework	F	SOC 2 Type II (report completed August 2026) plus signed Strict Data-Isolation Protocols addendum: tenant isolation, AES-256 at rest / TLS 1.3 in transit, audited zero-trust access, NIST SP 800-53 / ISO 27001 alignment.

E. Administrative & Incident Response Automation (4.1.5)

Requirement	Status	Comments
4.1.5.1 Automated remediation (search & destroy)	F	Global clawback across all 22,000 mailboxes within seconds; no manual approval required; SOAR-triggered workflows supported.
4.1.5.2 RBAC	F	Multi-agency separation, delegated administration, agency-scoped log visibility, full audit logging of administrative access.

F. Vendor Submission Requirements (4.1.6)

Requirement	Status	Comments
4.1.6.1 Architecture verification statement	F	Provided in Section 3.1, including the mail-flow diagram and architectural narrative. US data residency confirmed.
4.1.6.2 Compliance verification	F	Pathway C; SOC 2 Type II report provided with bid (Section 6.1).
4.1.6.3 Deployment timeline (<24 hours)	F	Confirmed in Section 9; no disruption to active State communications.
4.1.6.4 Pricing structure	F	Flat annual per-mailbox SaaS subscription, all-inclusive (Section 10).

Section 12: References

StrongestLayer is actively deployed in public-sector and education organizations with environments comparable to WVOT. To protect the privacy of our customers' personnel, detailed government and public-sector reference contacts will be furnished upon request once StrongestLayer's bid is shortlisted or accepted for award.

Section 13: Exceptions

None. StrongestLayer Inc. takes no exceptions to, and proposes no clarifications or modifications of, any requirement, term, or condition of CRFQ OOT2700000005. The proposed solution fully meets every mandatory specification, and StrongestLayer is prepared to execute the resulting contract as written.

Section 14: Insurance

StrongestLayer Inc. maintains, and will maintain for the life of the contract, insurance meeting or exceeding the required levels:

Commercial General Liability — at least $1,000,000 per occurrence.

Cyber Liability / Data Breach — at least $2,000,000 per occurrence.

Professional Liability (Errors & Omissions) — maintained for technology errors, omissions, and negligent acts.

Certificates of insurance will be provided prior to contract award, with the State named as required, and updated certificates furnished as policies renew.

Section 15: Required Forms & Acknowledgements

StrongestLayer will submit the following completed and signed solicitation documents with its bid in wvOASIS:

- Designated Contact, Certification and Signature page (signed).
- Addendum Acknowledgement Form (acknowledging all issued addenda).
- Purchasing Affidavit (no-debt certification, notarized).
- Pricing Pages / Exhibit A with unit pricing entered ($9.00 Year 1; $8.00 Years 2–4).
- Architecture verification statement with mail-flow diagram (Spec 4.1.6.1 — included in Section 3.1); Palo Alto NGFW no-conflict confirmation per Addendum No. 1, Q22 (Section 8).
- SOC 2 Type II report and Strict Data-Isolation Protocols addendum (Pathway C).
- Certificate of Good Standing and SAM.gov registration (supplemental).

End of Bid Response · StrongestLayer Inc. · CRFQ OOT2700000005 · August 2026

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:

Vendor Name : StrongestLayer Inc.

Address : 95 3rd St, 2nd Floor

Street :

City : San Francisco

State : CA **Country :** USA **Zip :** 94103

Principal Contact : Karen Letain

Vendor Contact Phone: 1-469-288-7477 **Extension:**

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

Vendor Signature X  **FEIN#** 92-0536529 **DATE** 08/18/2026

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

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

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

SCHEDULE OF EVENTS

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

	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

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

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

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

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

City :

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

Principal Contact :

Vendor Contact Phone: **Extension:**

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

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

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

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

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

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

Comm Code	Manufacturer	Specification	Model #
43230000			

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

SCHEDULE OF EVENTS

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

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

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

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

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

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

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

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

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

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

Submitted emails should have the solicitation number in the subject line. Question Submission Deadline: Tuesday August 11, 2026 @ 3:00 p.m.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GENERAL TERMS AND CONDITIONS:

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

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

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

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

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

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

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

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

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

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

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

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

[✔] Term Contract

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

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

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

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

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

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

[ ] the contract will continue for _____ years;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[ ]

[ ]

[ ]

[ ]

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

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

Vendor must maintain:

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

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

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

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

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

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

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

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

[ ]

[ ]

[ ]

[ ]

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

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

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

[ ] _____ for _____.

[ ] Liquidated Damages Contained in the Specifications.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Karen Letain, Chief Commercial Officer

(Address) 95 3rd St, 2nd Floor, San Francisco, CA 94103

(Phone Number) / (Fax Number) 1-469-288-7477 / N/A

(email address) karen@strongestlayer.ai

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

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

StrongestLayer Inc.

(Company)

(Signature of Authorized Representative)

Karen Letain, Chief Commercial Officer 08/18/2026

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

1-469-288-7477

(Phone Number) (Fax Number)

karen@strongestlayer.ai

(Email Address)

SPECIFICATIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. GENERAL REQUIREMENTS:

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

4.1.1 Core Architectural Requirements (Non-Gateway).

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

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

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

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

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

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

4.1.2 Gemini & Workspace Functional Integration

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

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

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

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

4.1.3 Technical & Threat Protection Capabilities

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

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

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

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

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

4.1.4 Compliance, Certifications, & Data Security

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

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

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

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

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

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

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

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

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

4.1.5 Administrative & Incident response Automation

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

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

4.1.6 Vendor Submission Requirements

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

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

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

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

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

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

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

7.0 CONTRACT AWARD:

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

7.2 Pricing Pages: Vendor should complete the Pricing Pages by providing the license cost. Vendor should complete the Pricing Pages in their entirety as failure to do so may result in Vendor's bids being disqualified.

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

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

8.0 ORDERING AND PAYMENT:

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

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

9.0 DELIVERY AND RETURN:

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

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

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

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

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

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

10.0 VENDOR DEFAULT:

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

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

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

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

10.1.4 Failure to remedy deficient performance upon request.

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

10.2.1 Immediate cancellation of the Contract.

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

10.2.3 Any other remedies available in law or equity.

11.0 MISCELLANEOUS:

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

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

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

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

Contract Manager: _____
Telephone Number: _____
Fax Number: _____
Email Address: _____

APPENDIX A:

SOFTWARE AS A SERVICE ADDENDUM

Software as a Service Addendum

1. Definitions:

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

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

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

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

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

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

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

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

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

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

Restricted data means personal data and non-public data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

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

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

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

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

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

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

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

14. Security:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

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

AGREED:

Name of Agency:_____	Name of Vendor: StrongestLayer Inc.
Signature:_____	Signature: 
Title:_____	Title: Chief Commercial Officer
Date:_____	Date: 08/18/2026

Appendix A

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

Name of Service Provider/Vendor: _____

Name of Agency:_____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐
2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐
3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐
5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

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

   Name: _____

   Email address: _____

   Phone Number: _____ _____

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)

[X]	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

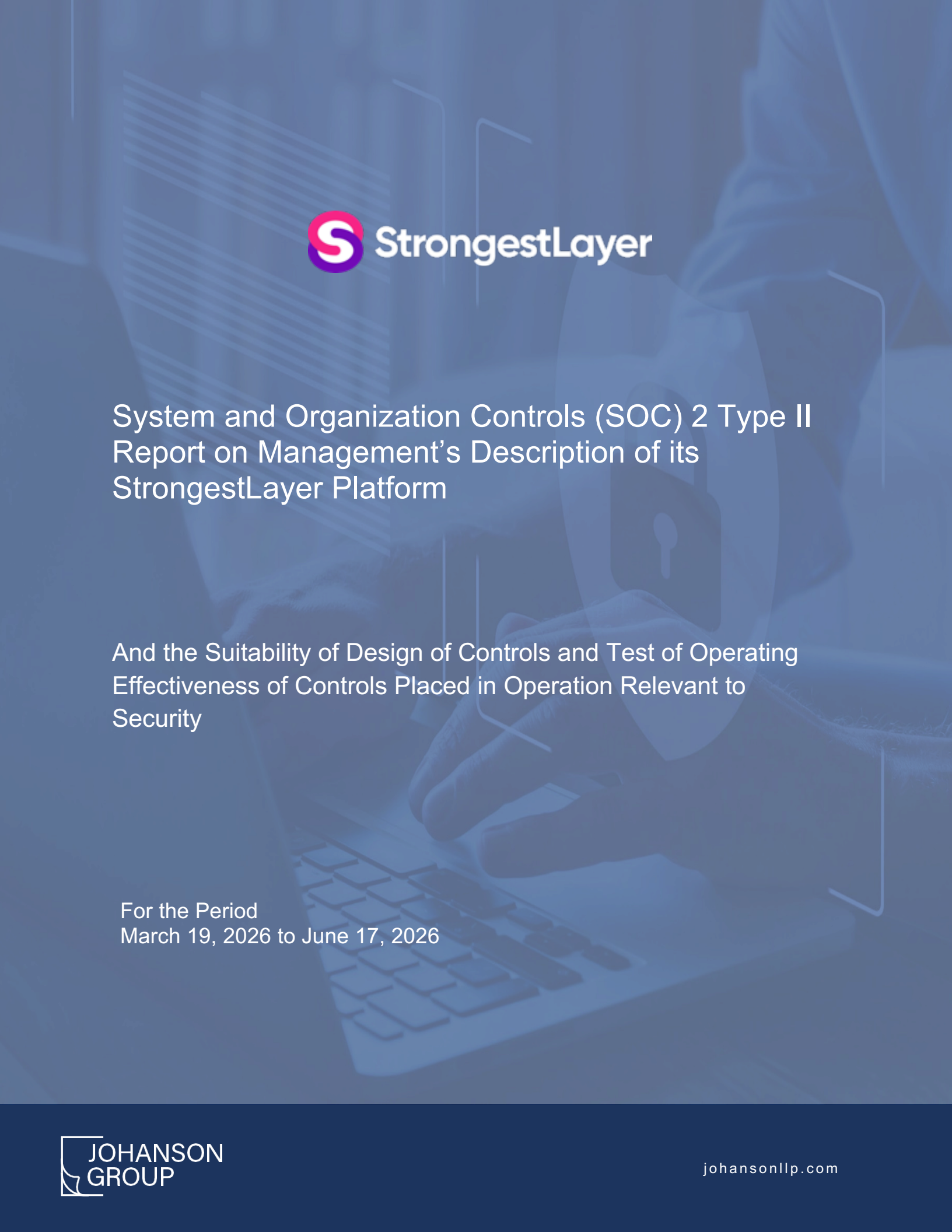
I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information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

StrongestLayer Inc.
Company

Authorized Signature

08/18/2026
Date

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



StrongestLayer

System and Organization Controls (SOC) 2 Type II Report on Management's Description of its StrongestLayer Platform

And the Suitability of Design of Controls and Test of Operating Effectiveness of Controls Placed in Operation Relevant to Security

For the Period
March 19, 2026 to June 17, 2026

JOHANSON GROUP

johansonllp.com

Table of Contents

Section I
Independent Service Auditor's Report

I. Independent Service Auditor's Report

StrongestLayer, Inc.

Scope

We have examined StrongestLayer, Inc.'s accompanying description of its StrongestLayer Platform (system) titled "Description of StrongestLayer" throughout the period March 19, 2026 to June 17, 2026(description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 19, 2026 to June 17, 2026, to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

StrongestLayer, Inc. uses a subservice organization, to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at StrongestLayer, Inc., to achieve StrongestLayer, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents StrongestLayer, Inc.'s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of StrongestLayer, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at StrongestLayer, Inc. to achieve StrongestLayer, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents StrongestLayer, Inc.'s controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of StrongestLayer, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

StrongestLayer, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements were achieved. StrongestLayer, Inc. has provided an assertion titled "Assertion of StrongestLayer, Inc.'s Management" (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. StrongestLayer, Inc. is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents StrongestLayer, Inc.'s StrongestLayer platform (system) that was designed and implemented throughout the period March 19, 2026 to June 17, 2026 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period March 19, 2026 to June 17, 2026, to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of StrongestLayer, Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period March 19, 2026 to June 17, 2026, to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of StrongestLayer, Inc.'s controls operated effectively throughout the period.

Restricted Use

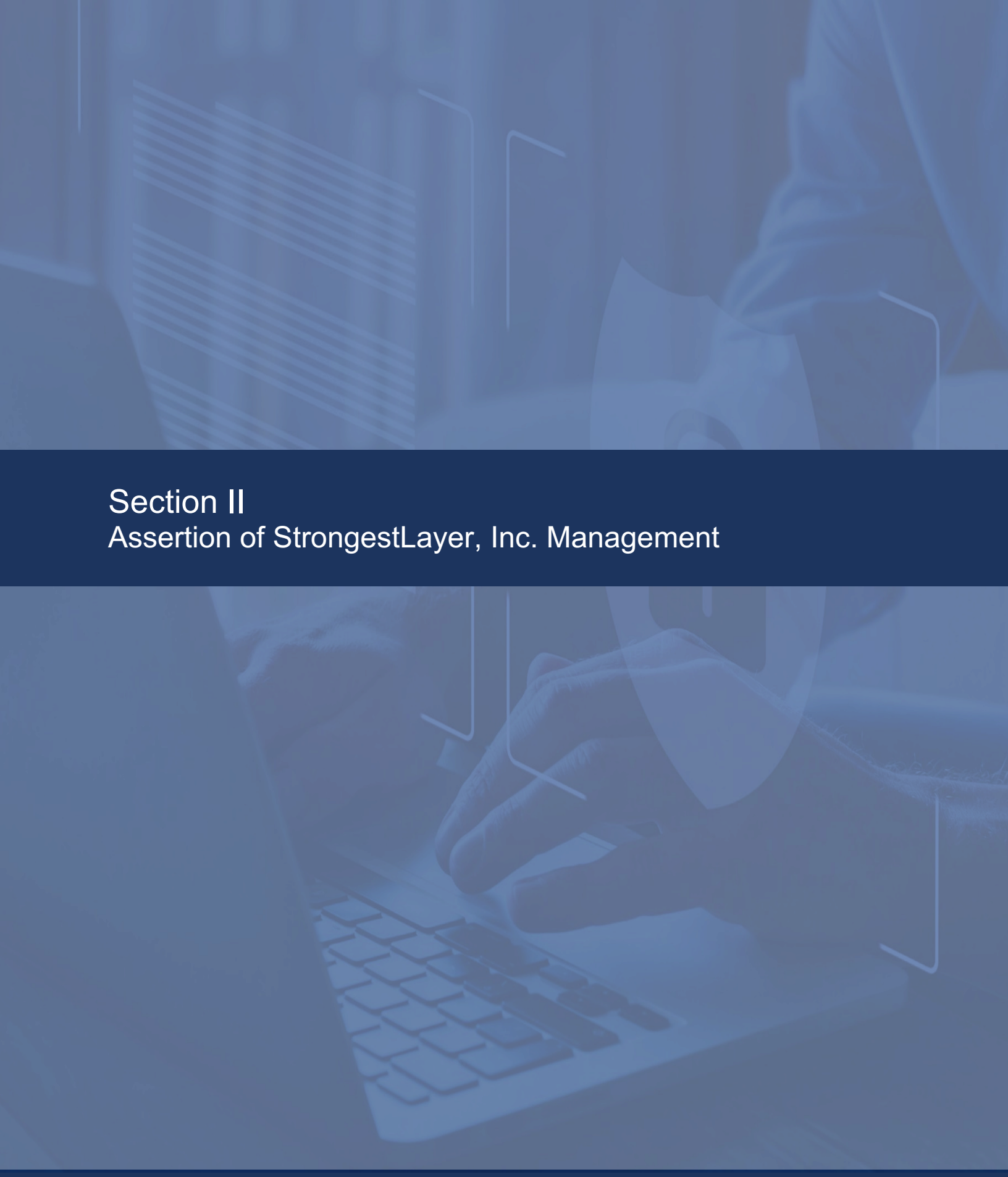
This report, including the description of tests of controls and results thereof in the section of our report titled "Description of Test of Controls and Results Thereof" is intended solely for the information and use of StrongestLayer, Inc.; user entities of StrongestLayer, Inc.'s StrongestLayer during some or all of the period March 19, 2026 to June 17, 2026, business partners of StrongestLayer, Inc. subject to risks arising from interactions with the StrongestLayer, Inc.'s processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

JohansonGroup LLP

Colorado Springs, Colorado
August 7, 2026



Section II
Assertion of StrongestLayer, Inc. Management

II. Assertion of StrongestLayer, Inc. Management

We have prepared the accompanying description of StrongestLayer, Inc.'s "Description of StrongestLayer Platform" for the period March 19, 2026 to June 17, 2026, (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about StrongestLayer, Inc.'s StrongestLayer platform (system) that may be useful when assessing the risks arising from interactions with StrongestLayer, Inc.'s system, particularly information about system controls that StrongestLayer, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

StrongestLayer, Inc. uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at StrongestLayer, Inc., to achieve StrongestLayer, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents StrongestLayer, Inc.'s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of StrongestLayer, Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls StrongestLayer, Inc., to achieve StrongestLayer, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents StrongestLayer, Inc.'s controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of StrongestLayer, Inc.'s controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents StrongestLayer, Inc.'s StrongestLayer Platform (system) that was designed and implemented throughout the period March 19, 2026 to June 17, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period March 19, 2026 to June 17, 2026, to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of StrongestLayer, Inc.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period March 19, 2026 to June 17, 2026, to provide reasonable assurance that StrongestLayer, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of StrongestLayer, Inc.'s controls operated effectively throughout that period.

StrongestLayer, Inc. Management
August 7, 2026

Section III
Description of StrongestLayer Platform

III. Description of StrongestLayer Platform

Company Background

StrongestLayer Inc. was incorporated in the State of Delaware in 2023 with the mission of protecting organizations from the rising wave of AI-generated email threats that bypass traditional security defenses. The company was founded by cybersecurity veterans with over 25 years of experience building security architectures at organizations including Proofpoint, FireEye, and Mandiant.

StrongestLayer is a fully remote organization with team members distributed across multiple geographies. The company operates without a centralized physical office, leveraging cloud-based collaboration tools and secure remote access infrastructure to support its workforce of approximately 25 to 30 employees and contractors.

In 2024, StrongestLayer secured $5.2 million in seed funding led by Sorenson Capital, with participation from strategic investors including Inovia Capital. This funding supports continued research and development of the company's AI-native email security platform and go-to-market expansion.

Industries served by StrongestLayer include Financial Services, Legal Services, Healthcare, Technology, and Managed Security Service Providers (MSSPs). The company's platform is deployed by mid-market and enterprise organizations seeking to defend against sophisticated phishing, business email compromise (BEC), and AI-generated threats that evade legacy Secure Email Gateways (SEGs) and native cloud email protections.

Services Provided

StrongestLayer provides AI-native email security services that protect organizations from sophisticated phishing, business email compromise (BEC), credential harvesting, and AI-generated email threats that bypass legacy defenses, including Microsoft E5 native protections, Proofpoint, Mimecast, and other Secure Email Gateways.

The StrongestLayer Email Security Platform is a multi-tenant software-as-a-service (SaaS) application that facilitates the detection, investigation, and triage of email-borne threats using proprietary large language model (LLM) based reasoning. The platform’s core detection engine, TRACE (Threat Reasoning and AI Correlation Engine), analyzes inbound email threats through five pillars:

- Intent Analysis – Determines the underlying purpose of an email by reasoning about its content, context, and behavioral signals.
- Anomaly Detection – Identifies deviations from established communication patterns and sender behaviors.
- Deception Scoring – Evaluates the degree to which an email employs social engineering, impersonation, or manipulation techniques.
- Harm Prediction – Assesses the potential organizational impact if a recipient interacts with the threat.
- Risk-Adjusted Triage – Prioritizes threats based on composite risk scores and delivers actionable case files to security teams.

The platform operates on a zero-memory architecture, processing email data in real time without persisting email content after threat assessment is complete. This design minimizes data exposure and supports compliance with data minimization principles.

Key services delivered through the platform include:

- Real-time threat detection and blocking of malicious emails before they reach end users.

- Automated threat investigation that produces complete case files with evidence, risk scores, and recommended actions for each detected threat.
- Security Operations Center (SOC) integration, reducing alert volume requiring manual investigation by more than 80% and reducing average triage time from 25 minutes to approximately 2 minutes per alert.
- API-based deployment that integrates with existing email infrastructure in approximately 15 minutes, with no MX record changes required.
- Continuous monitoring and detection updates powered by ongoing threat intelligence research.

Information is shared with customer organizations through the StrongestLayer web portal, admin portal, API integrations, and email notifications delivered over encrypted (TLS) connections.

Principal Service Commitments and System Requirements

StrongestLayer designs its processes and procedures related to the StrongestLayer Email Security Platform to meet its objectives for email security services. Those objectives are based on the service commitments that StrongestLayer makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that StrongestLayer has established for the services. Security commitments to user entities are documented and communicated in Master Service Agreements (MSAs), Service Level Agreements (SLAs), and other customer agreements, as well as in the description of the service offering provided online.

Security Commitments

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the StrongestLayer platform that restrict system access based on role and enforce the principle of least privilege across all platform components.
- Use of encryption technologies to protect customer data both in transit (TLS 1.2+) and at rest (AES-256 via AWS KMS-managed keys).
- A zero-memory data architecture that processes email content in real time without persisting customer email data after threat analysis is complete.
- API-based integration that requires no changes to customer email routing (no MX record modifications), minimizing the attack surface of deployment.

StrongestLayer establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the company's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the StrongestLayer Email Security Platform.

Components of the System

Infrastructure

The platform is hosted entirely on Amazon Web Services (AWS), leveraging AWS's Infrastructure as a Service (IaaS) offering to ensure scalability, reliability, and security. The infrastructure comprises the following key components:

- Amazon Elastic Compute Cloud (EC2) – Provides scalable virtual compute instances used to run core application workloads across multiple availability zones, ensuring operational resilience and redundancy. EC2 instances also host the self-managed Neo4j Graph Database deployment.
- Amazon Elastic Container Service (ECS) – Containerized workloads are deployed and orchestrated using AWS container services, enabling consistent, portable, and scalable deployment of application components across the infrastructure.
- AWS Lambda – Serverless compute functions are used to execute event-driven workloads and background processing tasks without the need to manage underlying server infrastructure.
- Amazon API Gateway – Serves as the managed entry point for all API traffic, enabling secure and scalable communication between clients and backend services.
- Amazon Simple Storage Service (S3) – Used for durable and scalable object storage, including hosting of the customer-facing web portal and admin portal as well as storage of application data, logs, and other assets.
- Amazon Relational Database Service (RDS) – Provides managed relational database instances to support structured data storage and retrieval requirements of the platform.
- Amazon DynamoDB – A fully managed NoSQL database service used for high-throughput and low-latency data access requirements.
- Amazon ElastiCache – Provides in-memory caching to improve application performance and reduce database load for frequently accessed data.
- Amazon Simple Queue Service (SQS) – Managed message queuing service used to decouple application components and facilitate asynchronous processing of workloads.
- Neo4j Graph Database – A self-hosted graph database deployed on EC2 instances used to manage and query complex, relationship-oriented data structures within the platform.
- Amazon Virtual Private Cloud (VPC) – Used to logically isolate the platform's infrastructure within a private, dedicated network, controlling routing, gateways, and network segmentation across all components.
- AWS Security Groups – Act as virtual firewalls to control inbound and outbound traffic at the instance level, enforcing the principle of least-privilege network access across all services.
- AWS Web Application Firewall (WAF) – Protects the customer-facing web portal, admin portal, and API endpoints from common web-based threats, including SQL injection, cross-site scripting, and other OWASP Top 10 vulnerabilities.
- Amazon GuardDuty – A threat detection service that continuously monitors AWS accounts and workloads for malicious activity and unauthorized behavior.
- Amazon Inspector – An automated vulnerability management service used to continually scan the infrastructure for software vulnerabilities and unintended network exposure.

Software

The system leverages a combination of modern frameworks and programming languages to deliver its services. The primary software components include:

- Next.js – Front-end framework used to build and serve the customer-facing web portal and admin portal, providing a responsive, dynamic, and performant user interface.
- Node.js – Server-side runtime used to power the backend of the web application layer, handling API requests, business logic, and communication between the frontend and underlying services.
- Python – The primary backend programming language for the platform's core service layer, facilitating robust server-side operations including data processing, business logic execution, and serverless function implementations running on AWS Lambda.
- Amazon CloudWatch – Used for continuous monitoring, logging, and alerting across the platform's AWS infrastructure and application components. CloudWatch provides visibility into system health, performance metrics, and operational events, enabling timely detection and response to anomalies.
- GitHub Actions – Powers the platform's CI/CD pipelines, automating the build and deployment of application code. All changes to production and non-production environments are deployed through structured, version-controlled pipeline workflows.

People

StrongestLayer has a staff of approximately 25 to 30 employees (via EOR) and contractors organized in the following functional areas:

- Executive Leadership. The Chief Executive Officer (CEO), Alan Lefort, provides overall strategic direction, oversees company operations, and is responsible for governance, compliance, and board-level reporting. The CEO is supported by a leadership team with direct oversight of engineering, security, and go-to-market functions.
- Engineering and Product Development. Led by the Chief Technology Officer (CTO), Muhammad Rizwan, this team is responsible for the design, development, testing, and deployment of the StrongestLayer Email Security Platform. The engineering team includes software developers, data scientists, AI/ML engineers, and DevOps personnel who build and maintain the platform's detection engine, API infrastructure, web portals, and CI/CD pipelines.
- Information Security. Led by the Head of Information Security, Ali Raza, this function is responsible for security policy development and enforcement, access control management, vulnerability management, incident response, vendor risk assessment, security awareness training, and compliance monitoring. The information security team works closely with engineering to ensure secure-by-design development practices are followed.
- Sales and Customer Success. This team manages customer relationships, onboarding, and ongoing account support. Customer-facing personnel coordinate platform deployment, provide technical assistance, and serve as the primary point of contact for service-related inquiries.
- Threat Research. Dedicated researchers who continuously analyze emerging email threat vectors, AI-generated attack techniques, and adversary tactics to inform and improve the platform's detection capabilities.

All personnel are required to complete security awareness training upon onboarding and on an annual basis thereafter. Background checks are performed for employees as a component of the hiring process.

Data

Data processed by the StrongestLayer Email Security Platform includes the following categories:

- Inbound email metadata and content – The platform processes email headers, body content, sender/recipient information, embedded URLs, and attachment metadata to perform real-time threat analysis. Under the platform's zero-memory architecture, email content is analyzed in memory and is not persisted after the threat assessment is complete.
- Threat detection data – Results of the TRACE detection engine's analysis, including intent scores, anomaly indicators, deception scores, harm predictions, and composite risk ratings. This data is retained to support threat investigation, case file generation, and historical reporting for customers.
- Customer configuration data – Organizational settings, user roles, notification preferences, API integration credentials, and deployment configuration required to operate the service for each customer tenant.
- User authentication data – Account credentials, session tokens, and multi-factor authentication records for platform users accessing the web portal and admin portal.
- Audit and system logs – Application logs, API access logs, infrastructure monitoring data, and security event logs generated by AWS CloudWatch, GuardDuty, and other monitoring tools. These logs are retained for operational troubleshooting, security monitoring, and compliance purposes.
- Reporting and analytics data – Aggregated threat metrics, detection statistics, and performance data presented through platform dashboards and exported reports.

All data in transit is encrypted using TLS 1.2 or higher. Data at rest is encrypted using AES-256 encryption with AWS KMS-managed keys. Access to customer data is restricted to authorized personnel on a need-to-know basis in accordance with the company's access control policies.

Processes and Procedures

Formal policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to StrongestLayer's policies and procedures that define how services should be delivered.

Physical Security

StrongestLayer is a fully remote organization with no company-owned or leased physical office facilities or data centers. All production infrastructure is hosted entirely on Amazon Web Services (AWS).

Physical security controls for the underlying compute, storage, and networking infrastructure are managed by AWS in accordance with AWS's own security policies and certifications, including SOC 2 Type II. Physical security controls will be carved out of StrongestLayer's SOC 2 report and addressed through AWS's complementary subservice organization controls as described in the Subservice Organizations section of this document.

StrongestLayer monitors the physical security posture of its subservice organization (AWS) by reviewing AWS's SOC 2 report on an annual basis and evaluating any identified exceptions or findings.

Logical Access

StrongestLayer employs role-based access control (RBAC) and requires all users of the system to be identified and authenticated prior to accessing any system resources. Access to production infrastructure, application systems, and internal tools is governed by the company's Information Security Policy (Acceptable Use Policy) managed in Vanta.

Authentication and Access Controls

- All employees access corporate resources and cloud services through Google Workspace, which serves as the company's identity provider for Single Sign-On (SSO).
- Multi-factor authentication (MFA) is required for all cloud-based services and infrastructure access, including AWS console access, GitHub, and the Vanta compliance platform.
- Access to the AWS production environment is restricted to authorized engineering and DevOps personnel. AWS IAM policies enforce the principle of least privilege, and administrative access requires MFA.
- Access to application source code repositories on GitHub is restricted to authorized development team members. Branch protection rules are enforced on all production branches.
- Remote access to internal infrastructure is secured through Tailscale, a zero-trust networking solution that authenticates users and devices before granting access to private network resources.

Provisioning and Deprovisioning

- New employee access is provisioned based on predefined role-based access templates. The employee's manager approves the access scope prior to the employee's start date.
- Upon termination, access to all corporate systems is revoked within 24 hours. Account deactivation is tracked through the Vanta platform, which monitors for timely offboarding completion.

Access Reviews

- Access reviews for critical systems are conducted on a quarterly basis. The CTO reviews privileged access to production infrastructure and requests modifications based on this review.
- Vanta continuously monitors access configurations across integrated systems and alerts the security team to any deviations from established access policies.

Computer Operations - Backups

Customer and system data is backed up and managed by the company's DevOps team. Backup procedures are defined as part of the company's Business Continuity and Disaster Recovery (BC/DR) Plan, which establishes recovery objectives, responsibilities and restoration processes to ensure continuity of critical services in the event of a disruption.

Backup Storage and Retention

Backups are maintained within AWS with physical access to the underlying infrastructure restricted in accordance with AWS's applicable security policies. In addition to cloud-hosted copies, backups are also downloaded and retained offline, providing an additional layer of redundancy and recoverability independent of AWS availability.

Recovery Objectives

The BC/DR Plan defines formal Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical system assets. For core AWS-hosted services, the defined RTO is 2 hours, and the RPO is 15 minutes, reflecting the criticality of production service availability to customers.

Disaster Recovery Testing

The company has conducted a tabletop exercise to walk through disaster recovery scenarios, validate the BC/DR Plan, and assess the readiness of key personnel and defined procedures. A full technical restoration test of backup recovery processes has not yet been performed. The company intends to conduct formal backup restoration testing on an annual basis going forward in alignment with the requirements defined in the BC/DR Plan.

Backup Exception Handling

In the event of a backup exception or failure, DevOps personnel perform troubleshooting to identify the root cause and re-run the backup job immediately or as part of the next scheduled backup cycle.

Computer Operations - Availability

StrongestLayer has implemented incident response policies and procedures to guide personnel in identifying, reporting, and responding to information technology incidents and security events. The Incident Response Plan defines roles, responsibilities, escalation procedures, and communication protocols for security incidents of varying severity levels.

Monitoring and Alerting

- Amazon CloudWatch provides continuous monitoring of system health, performance metrics, and operational events across all AWS infrastructure components. Alerts are configured to notify the DevOps and security teams of anomalies or threshold breaches.
- Amazon GuardDuty provides automated threat detection by continuously monitoring for malicious activity and unauthorized behavior within the AWS environment.
- Amazon Inspector performs automated vulnerability scanning of infrastructure for software vulnerabilities and unintended network exposure.
- Vanta provides continuous compliance monitoring, tracking the status of security controls and alerting the security team to any control failures or deviations.

Capacity Management

StrongestLayer's infrastructure leverages AWS auto-scaling capabilities to dynamically adjust compute and storage resources in response to workload demands. The DevOps team monitors capacity utilization through CloudWatch dashboards and evaluates the need for additional infrastructure capacity in response to customer growth.

Patch Management

The company follows a defined patch management process to ensure production systems are updated in accordance with vendor-recommended patches and security advisories. Critical and high-severity patches are evaluated and applied within defined SLA windows. Amazon Inspector continuously scans for known vulnerabilities, and Dependabot monitors application dependencies for security updates as part of the CI/CD pipeline.

Change Control

StrongestLayer maintains a documented Secure Software Development Life Cycle (SDLC) policy that governs how application and infrastructure changes are designed, developed, tested, and deployed. The policy establishes principles for secure-by-design and privacy-by-design development, enforces segregation of development, staging, and production environments, and requires that no single individual can develop, approve, and deploy a change without appropriate oversight.

Change Initiation and Tracking

All changes, including new features, bug fixes and infrastructure updates, are initiated and tracked using JIRA, the company's ticketing system. Each change request is documented with a description of the change and approval status before progression to production.

Version Control and Code Review

GitHub serves as the version control platform for all application source code. The engineering organization is structured around small, module-owning pods of two to three engineers and review responsibility is assigned by module and repository ownership. Each repository is owned by a pod and pull requests are reviewed by a member of the owning pod or another authorized engineer.

Branch protection rules are enforced on all protected branches ensuring that no code can be merged directly without passing through a formal pull request process. Regardless of pod size or the number of active contributors, every pull request to a protected branch must receive at least one independent approving review from an engineer other than the author before it can be merged. Self-approval and self-merge are prohibited and are enforced through branch protection.

Where a repository is temporarily reduced to a single active contributor (for example, due to a staffing change), the independent-review requirement remains fully in force. An approving review is obtained from another engineer with access to the repository, or an interim reviewer — the Engineering Manager, CTO, or a GitHub administrator's designee — is assigned until a second contributor is available. Changes are never merged to a protected branch without independent approval. These requirements are defined in the company's Secure Development Policy and the associated Version Control Procedure.

CI/CD and Deployment Pipelines

Deployments to all environments are executed exclusively through GitHub Actions pipelines. The pipelines integrate the following automated security and code quality tools as mandatory gates that must pass successfully before any code can be deployed:

- Dependabot – Continuously monitors application dependencies for known vulnerabilities.
- Bandit – A static analysis tool that scans Python source code for common security issues and vulnerabilities prior to deployment.
- Ruff – A Python linter used to enforce code quality and style standards across the codebase as part of the pipeline execution.
- mypy – A static type checker for Python that validates type correctness across the codebase, reducing the risk of runtime errors and logic flaws reaching production.

Code can only be deployed to production after a pull request has been reviewed and approved and all pipeline checks, including the above, have executed successfully. This enforces a structured, auditable, and automated approval gate that prevents unreviewed or non-compliant code from reaching production.

Testing and Acceptance

Prior to deployment, changes and features must pass testing cycles. Any bug identified is logged and tracked until it is remediated.

Segregation of Environments

Development, staging, and production environments are logically segregated to ensure that testing and development activities do not impact live customer data or system availability.

Data Communications

Network Security

AWS Security Groups act as virtual firewalls to control inbound and outbound network traffic at the instance level, enforcing the principle of least-privilege network access. All production resources are deployed within Amazon Virtual Private Cloud (VPC), which provides logical network isolation and controlled routing between components.

AWS Web Application Firewall (WAF) protects the customer-facing web portal, admin portal, and API endpoints from common web-based threats including SQL injection, cross-site scripting, and other OWASP Top 10 attack vectors. Administrative access to network and firewall configurations is restricted to authorized DevOps personnel.

Encryption

All data in transit is encrypted using TLS 1.2 or higher. Data at rest is encrypted using AES-256 encryption with AWS KMS-managed keys. All API communications between customers and the platform are conducted over HTTPS-secured connections.

Remote Access

Authorized employees access internal infrastructure through Tailscale, a zero-trust networking solution that authenticates users and devices before granting access to private network resources. All remote access requires multi-factor authentication.

Penetration Testing

Penetration testing is conducted annually by a qualified third-party vendor. The most recent external infrastructure penetration test was performed by Evoionos and completed in March 2026. The test covered 7 domains and 2 IP addresses. Four vulnerabilities were identified, all of which were remediated and verified as closed prior to the conclusion of the engagement.

Vulnerability Scanning

Amazon Inspector provides continuous automated vulnerability scanning of the production infrastructure. Dependabot monitors application dependencies for known vulnerabilities as part of the CI/CD pipeline. The company has published a Vulnerability Disclosure Policy (SL-POL-VDP-001) that establishes processes for receiving, evaluating, and remediating security vulnerabilities reported by external researchers, with defined response commitments by severity level.

The Applicable Trust Services Criteria and The Related Controls

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage, and ii. systems that use electronic information to process, transmit, or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of StrongestLayer's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of StrongestLayer's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices.

Specific control activities that StrongestLayer has implemented in this area are described below:

- A formally documented Information Security Policy (Acceptable Use Policy) communicates entity values and behavioral standards to all personnel. The policy is maintained in Vanta and reviewed at least annually.
- All employees are required to acknowledge the company's information security policies upon onboarding and annually thereafter, confirming they have read and understand their responsibilities for adhering to company policies and procedures.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties is included as part of the onboarding process.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

StrongestLayer's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes consideration of the competence levels for particular positions and how those levels translate into requisite skills and knowledge.

Specific control activities that StrongestLayer has implemented in this area are described below:

- Management has considered the competence levels for particular positions and translated required skills and knowledge levels into written position requirements and job descriptions.
- Security awareness training is provided to all personnel upon onboarding and on an annual basis to maintain awareness of security threats, company policies, and individual responsibilities.
- The company's founding team brings over 25 years of experience building security architectures at leading cybersecurity organizations including Proofpoint, FireEye, and Mandiant, establishing a strong foundation of security competence across the organization.

Management's Philosophy and Operating Style

StrongestLayer's management philosophy and operating style encompass a broad range of characteristics. These include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, security operations, and personnel.

Specific control activities that StrongestLayer has implemented in this area are described below:

- Management periodically discusses the regulatory and industry changes affecting the cybersecurity and email security landscape, including emerging AI-generated threat vectors and evolving compliance requirements.
- Executive leadership meetings are held regularly to discuss major initiatives, product roadmap priorities, security posture, and operational issues that affect the business.

- The company maintains a compliance-first operating philosophy, leveraging the Vanta platform for continuous monitoring of security controls and proactive identification of compliance gaps.

Organizational Structure and Assignment of Authority and Responsibility

StrongestLayer's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. The organizational structure has been developed to suit the company's size and the nature of its activities as an early-stage cybersecurity company.

Specific control activities that StrongestLayer has implemented in this area are described below:

- A clear organizational structure defines key areas of authority and responsibility across executive leadership, engineering, information security, and go-to-market functions.
- SOC 2 control ownership has been formally assigned across three responsible owners: the CEO (18 controls covering governance, HR, and board-level oversight), the CTO (37 controls covering infrastructure, SDLC, network, and encryption), and the Head of Information Security (25 controls covering security policy, access control, incident response, risk, training, and vendor management).
- The Board of Directors, consisting of 5 members including independent investor-appointed directors, provides governance oversight of the company's strategy, risk management, and compliance posture.

Human Resource Policies and Practices

StrongestLayer's success is founded on sound business ethics, reinforced with high standards of integrity and accountability. The company's human resources policies and practices relate to employee and contractor hiring, onboarding, training, evaluation, and termination activities.

Specific control activities that StrongestLayer has implemented in this area are described below:

- New employees (Via EOR) are required to complete security awareness training and acknowledge information security policies during the onboarding process.
- Background checks are performed for employees as part of the hiring process.
- Contractor agreements include confidentiality provisions and define security responsibilities and obligations.
- Employee and contractor termination procedures are in place to ensure timely revocation of system access. Access to all corporate systems is revoked within 24 hours of termination, tracked through the Vanta platform.

Risk Assessment Process

StrongestLayer's risk assessment process identifies and manages risks that could potentially affect the company's ability to provide reliable services to customer organizations. This ongoing process requires that management identify significant risks inherent in the company's products and services as they oversee their areas of responsibility.

StrongestLayer identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks. This process has identified risks resulting from the nature of the services provided, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, technology dependencies, or management personnel that could affect service delivery.
- Strategic risk – new AI-generated threat techniques, changing attack methodologies, evolving customer requirements, and shifts within the cybersecurity industry.
- Compliance risk – legal and regulatory changes affecting data protection, privacy, and security certification requirements.
- Technology risk – vulnerabilities in third-party dependencies, cloud infrastructure disruptions, or failures in detection model accuracy.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of StrongestLayer's system; as well as the nature of the components of the system result in risks that the criteria will not be met. StrongestLayer addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, StrongestLayer's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

The company utilizes the Vanta platform to continuously monitor the operational effectiveness of security controls and identify control failures or deviations in real time. Risk assessments are reviewed and updated at least annually by the security team, with findings reported to executive leadership for remediation prioritization.

Information and Communication Systems

Information and communication is an integral component of StrongestLayer's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

StrongestLayer uses the following communication systems and channels to support its operations:

- Slack is the primary internal communication platform, used for day-to-day team collaboration, operational discussions, security incident coordination, and dissemination of policy updates. A dedicated #soc2 channel is used for compliance-related communications.
- Google Workspace (Gmail, Google Drive, Google Calendar) provides email, document collaboration, and scheduling services for the organization.
- JIRA is used for project management, change tracking, and issue resolution across engineering and product teams.
- Vanta serves as the compliance management platform, providing automated evidence collection, control monitoring, policy management, and audit preparation capabilities.
- GitHub provides version control and CI/CD pipeline management, serving as the primary collaboration platform for engineering teams

Company-wide communications, including policy updates, security advisories, and organizational announcements, are distributed through Slack and email. Regular team meetings and all-hands sessions are conducted to discuss operational priorities, product updates, and compliance status.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. StrongestLayer's management performs monitoring activities to continuously assess the quality of internal controls over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures.

Continuous Monitoring

- Vanta provides automated, continuous monitoring of security controls across the organization's integrated systems. Control tests are executed automatically, and the security team is alerted to any failures or deviations from established policies.
- Amazon CloudWatch, GuardDuty, and Inspector provide continuous infrastructure monitoring for performance anomalies, security threats, and vulnerabilities.
- Endpoint compliance is monitored through the Vanta device monitoring agent, which tracks hard drive encryption status, screen lock settings, password manager deployment, and antivirus/EDR status across all company-managed devices.

Reporting and Remediation

- Control failures identified through Vanta are triaged by the security team and assigned to the responsible control owner (CEO, CTO, Head of Cloud Infrastructure or Director Security & Compliance) for remediation.
- A consolidated compliance punch list is maintained to track open remediation items, categorized by priority and effort level.
- Management reviews the overall compliance posture on a regular basis and reports to executive leadership on control effectiveness and remediation progress.

Changes to the System

Major Platform & Detection Changes (Apr 2025 – Mar 2026):

1. TRACE Engine – Verdict Mode Launch (Jul 2025) — TRACE, the core reasoning-based threat detection engine, was deployed in Verdict mode across all accounts. This marked the transition to a reasoning-based detection architecture.
2. PhishLLM (May–Jun 2025) — First basic version of the LLM-based phishing detection engine pushed to production, with ongoing model training and prompt tuning.
3. AI Advisor Redesign (Jun–Sep 2025) — Complete UI overhaul of the AI Advisor (Outlook add-in / digital security assistant), including new loading screens, safe/malicious email screens, report FP/FN, training quiz, and simulation email screens. New Marketplace listing published.
4. CISO Dashboard / ROI API (Sep 2025) — Development of ROI metrics API for the CISO dashboard.
5. Pendo Integration (Sep 2025) — Customer analytics and in-app engagement tool deployed in the new UI.
6. Slack Alerting Integration (Nov 2025) — Slack-based notification system for threat alerts deployed to production.
7. Group/OU Selection & Phased Rollouts (Dec 2025) — Admins can select Groups/Organizational Units for phased email security rollouts with user-level exclusion logic.
8. Multi-Domain Support (Azure AD / Entra ID) (Dec 2025) — Support for multiple domains under a single tenant.
9. POC Real-Time Digest Alerts (Dec 2025) — Real-time admin alert notifications during proof-of-concept deployments.

10. Improved Dashboard Filters (Dec 2025) — Customer-requested filter improvements.
11. Threat Hunt (Jan 2026) — New feature with Mailbox Hunt, Analyzed Emails, and Hunt History capabilities.
12. Trust Management (Jan 2026) — Deployed to staging.
13. Cost API & Provision Portal (Jan 2026) — Cost tracking API for POC and customer cost visibility.

Incidents

No significant incidents have occurred to the services provided to user entities since the last review date.

Criteria Not Applicable to the System

All Common Criteria/Security criteria were applicable to the StrongestLayer system.

Subservice Organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

StrongestLayer's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to StrongestLayer's services to be solely achieved by StrongestLayer's control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish its own internal controls to complement those of StrongestLayer.

Amazon Web Services (AWS) is StrongestLayer's sole subservice organization. AWS provides the Infrastructure as a Service (IaaS) platform on which the StrongestLayer Email Security Platform is hosted. The following complementary subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed-circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

StrongestLayer management monitors the subservice organization through the following procedures:

- Reviewing AWS's SOC 2 Type II attestation report on an annual basis to assess the design and operating effectiveness of AWS controls.

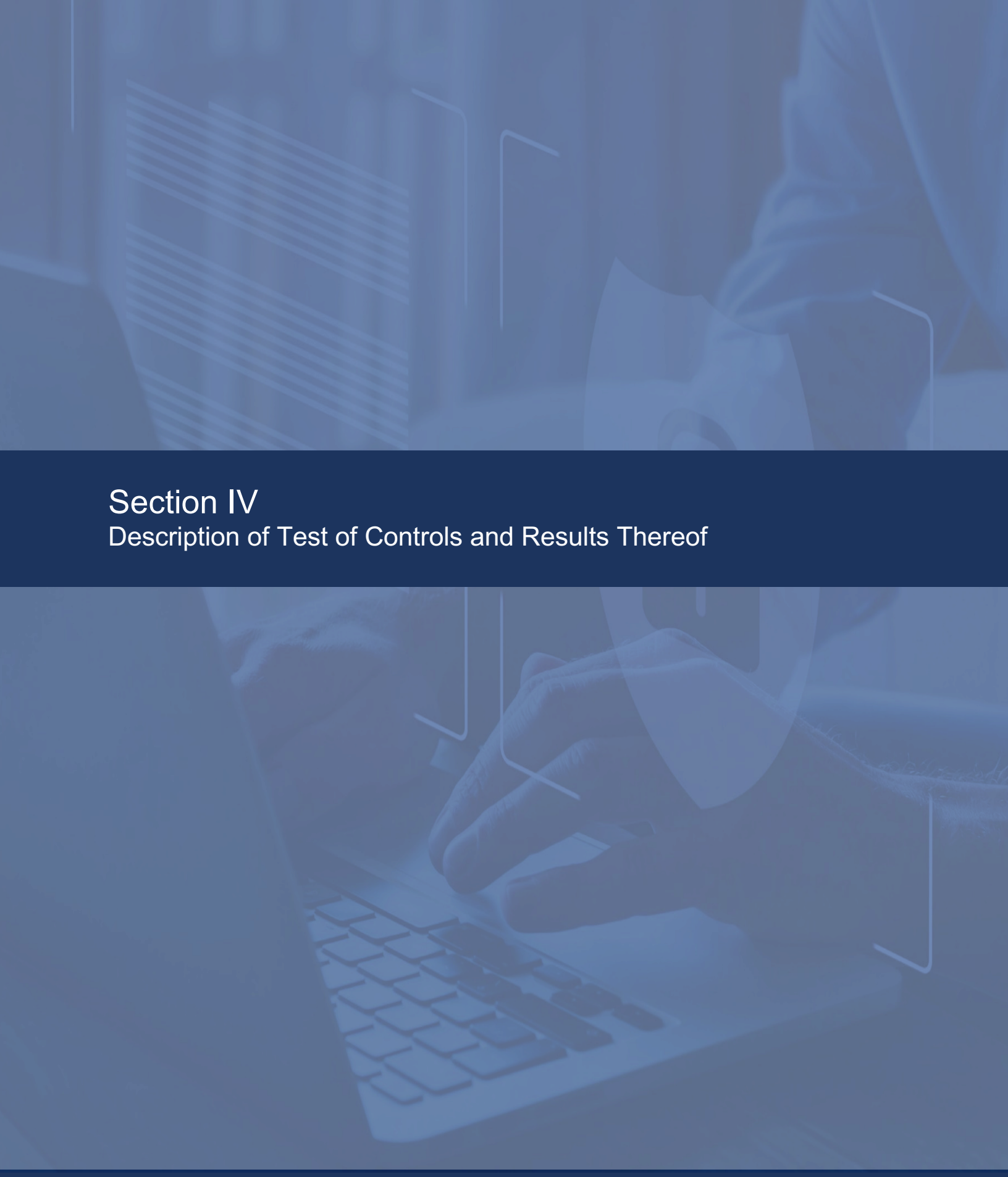
- Monitoring external communications, security advisories, and service health dashboards published by AWS.
- Evaluating the findings and exceptions reported in AWS's attestation reports for relevance to StrongestLayer's control environment.

Complementary User Entity Controls

StrongestLayer's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to StrongestLayer's services to be solely achieved by StrongestLayer's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of StrongestLayer.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met:

1. User entities are responsible for understanding and complying with their contractual obligations to StrongestLayer.
2. User entities are responsible for notifying StrongestLayer of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of StrongestLayer services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize StrongestLayer services.
6. User entities are responsible for providing StrongestLayer with a list of authorized users and promptly notifying StrongestLayer when user access should be revoked.
7. User entities are responsible for immediately notifying StrongestLayer of any actual or suspected information security breaches, including compromised user accounts or API credentials used for platform integrations.



Section IV
Description of Test of Controls and Results Thereof

IV. Description of Test of Controls and Results Thereof

Relevant trust services criteria and StrongestLayer, Inc.'s related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if StrongestLayer, Inc.'s controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, Trust Services Criteria, throughout the period March 19, 2026 to June 17, 2026.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of StrongestLayer, Inc. activities and operations, and inspection of StrongestLayer, Inc. documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson Group LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all StrongestLayer, Inc. controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The Company has a documented Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	1. Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. 2. Obtained a population of new hires across the entire audit period and selected a sample according to our sampling guidance. 3. Inspected and signed agreements for the selected sample of new hires during the audit period to determine whether it was acknowledged upon hiring.	No exceptions noted.
CC1.1.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	1. Obtained a population of new hires across the entire audit period and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that a background check was completed for the new hire(s) prior to their start date.	No exceptions noted.
CC1.1.3	The company management demonstrates a commitment to integrity and ethical values.	1. Obtained and inspected the Ethical Management Questionnaire to determine that it was signed by Company Management.	No exceptions noted.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.2	The company management demonstrates a commitment to integrity and ethical values.	1. Obtained and inspected the Ethical Management Questionnaire to	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
		determine that it was signed by Company Management.	
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The Company has a documented organization chart which outlines the roles, functional responsibilities and reporting lines for the entity personnel.	1. Obtained and inspected the Organization Chart to determine that reporting lines, authorities, and responsibilities.	No exceptions noted.
CC1.3.2	The company management demonstrates a commitment to integrity and ethical values.	1. Obtained and inspected the Ethical Management Questionnaire to determine that it was signed by Company Management.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Job skill requirements/qualifications are documented in job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and performance review processes.	1. Inquire with Management to confirm that job requirements are evaluated during the hiring process. 2. Obtain and inspect one sample of a job description to confirm that job requirements/skills are defined.	No exceptions noted.
CC1.4.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	1. Obtained a population of new hires across the entire audit period and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that a background check was completed for the new hire(s) prior to their start date.	No exceptions noted.
CC1.4.3	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they completed the Security Awareness training within the last year.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The Company Managers complete performance reviews for employees at least annually.	1. Obtained a population of current employees during the audit period and selected a sample according to our sampling guidance. 2. Inspected the performance review(s) for the selected sample of employees to determine that the performance review was conducted within the past year.	No exceptions noted.
CC1.5.2	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
		completed the Security Awareness training within the last year.	
CC1.5.3	The Company has a documented Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	1. Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. 2. Obtained a population of new hires across the entire audit period and selected a sample according to our sampling guidance. 3. Inspected and signed agreements for the selected sample of new hires during the audit period to determine whether it was acknowledged upon hiring.	No exceptions noted.
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The Company performs continuous control activity monitoring through the use of a GRC Platform or manual controls testing to ensure controls are operating effectively.	Inspected StrongestLayer, Inc.'s continuous control monitoring dashboard (or equivalent) to determine that the entity performs control monitoring to gain assurance that controls are in place and operating effectively.	No exceptions noted.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The entity has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees.	1. Obtained a population of new hires across the entire audit period and selected a sample according to our sampling guidance. 2. Inspected the evidence of acknowledgement of security policies for the selected new hires.	No exceptions noted.
CC2.2.2	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they completed the Security Awareness training within the last year.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected StrongestLayer, Inc.'s Master Service Agreement (MSA) or Terms of Service (TOS) to determine that the company and customer responsibilities are described in the agreements.	No exceptions noted.
CC2.3.2	The entity provides a process to external users for reporting security,	Inspected StrongestLayer, Inc.'s support page to determine that the	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	entity provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's objectives and are used as part of the annual risk assessment.	Inspected StrongestLayer, Inc.'s risk assessment to determine that the management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's objectives and are used as part of the annual risk assessment.	No exceptions noted.
CC3.1.2	The company conducts an internal control review annually to ensure controls are functioning as expected.	Inspected StrongestLayer, Inc.'s Vanta Dashboard to determine that the company conducts an internal control review annually to ensure controls are functioning as expected.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	As part of the risk assessment, vulnerabilities and threats are identified corresponding to risks. With vendors and partners needed to conduct business in the Cloud, these entities are analyzed for potential vulnerabilities. Risks are subsequently rated using a risk evaluation process and are documented in a risk register, along with mitigation strategies, for management review.	Inspected StrongestLayer, Inc.'s risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC3.2.2	A systems inventory is maintained that includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	Inspected StrongestLayer, Inc.'s systems inventory and determined that it is maintained and includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Management considers the potential for fraudulent activity as part of the annual risk review process.	Inspected StrongestLayer, Inc.'s risk assessment to determine that management considers the potential for fraudulent activity as part of the annual risk review process.	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	As part of the risk management process, management considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year and are formally documented.	Inspected StrongestLayer, Inc.'s risk assessment to determine that, as part of the risk management process, management considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year and are formally documented.	No exceptions noted.
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The Company continuously monitors to detect any security events, latency, network performance, and virtual server performance issues.	1. Inspected the entity's monitoring dashboard (or equivalent) to determine that the entity continuously monitors to detect any security events, latency, network performance, and virtual server performance issues.	No exceptions noted.
CC4.1.2	Capacity monitoring is performed to ensure that the use of resources is within acceptable limits and below maximum utilization for a resource.	Inspected StrongestLayer, Inc.'s monitoring dashboard to determine that capacity monitoring is performed to ensure that use of resources is within acceptable limits and below maximum utilization for a resource.	No exceptions noted.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Control owners perform an annual self-evaluation of the effectiveness of controls, which are reviewed for management action and/or input to the risk management process.	Inspected StrongestLayer, Inc.'s Annual Internal Control Self-Assessment to determine that control owners perform an annual self-evaluation of the effectiveness of controls, which are reviewed for management action and/or input to the risk management process.	No exceptions noted.
CC4.2.2	The entity provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected StrongestLayer, Inc.'s support page to determine that planned changes and updates are communicated as part of the development roadmap.	No exceptions noted.
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The Company makes changes as appropriate to address any identified risks. These issues are considered and prioritized as part of a regular development planning process. Assigned Control owners update	Inspected StrongestLayer, Inc.'s risk assessment to determine that the company makes changes as appropriate to address any identified risks. These issues are considered and prioritized as part of a regular	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	control activities to mitigate the risks identified during the annual risk assessment process.	development planning process. Assigned Engineering owners develop control activities to mitigate the risks identified during the annual risk assessment process.	
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis.	Inspected StrongestLayer, Inc.'s risk assessment to determine that assigned risk owners develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Information system security and management policies are formally documented and reviewed on an annual basis, which identifies information required to support the functioning of internal control and achievement of objectives.	Inspected StrongestLayer, Inc.'s information system security and management policies to determine that information system security and management policies are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC5.3.2	An employee sanction procedure is in place and documented within the employee handbook, communicating that an employee may be terminated for noncompliance with the handbook, code of conduct, or security policy.	Inspected StrongestLayer, Inc.'s information system security and management policies to determine that an employee sanction procedure is in place and documented within the employee handbook, communicating that an employee may be terminated for noncompliance with the handbook, code of conduct, or security policy.	No exceptions noted.
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC6.1.2	The in-scope systems and applications are configured to enforce minimum password requirements.	Inspected StrongestLayer, Inc.'s password configurations to determine that the in-scope systems and applications are configured to enforce minimum password requirements.	No exceptions noted.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	New hire access is granted based on job responsibility and is requested,	1. Obtained a population of new hires across the entire audit period and	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	documented, and authorized by management prior to the start date.	selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the new hire's access was properly approved prior to their start date.	
CC6.2.2	Access changes are properly approved.	1. Obtained a population of access changes across the entire audit period and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the access change was properly approved.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no access changes occurred during the review period.
CC6.2.3	Terminated user access rights are disabled by IT following termination notification from HR. All access changes, including terminations, are documented and tracked in the Help Desk ticket system.	1. Obtained a population of terminated users across the entire audit period and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the terminated user's access was properly removed in a timely manner.	No exceptions noted.
CC6.2.4	User access roles and privileges are reviewed and approved or updated by management on an annual basis.	Inspected StrongestLayer, Inc.'s annual user access review to determine that annual reviews of the entity's critical systems and associated user access rights were performed to ensure access was appropriate or to modify access where required.	No exceptions noted.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	User access roles and privileges are reviewed and approved or updated by management on an annual basis.	Inspected StrongestLayer, Inc.'s annual user access review to determine that annual reviews of the entity's critical systems and associated user access rights were performed to ensure access was appropriate or to modify access where required.	No exceptions noted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	The Company does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is Carved Out	Control is implemented and maintained by subservice organizations.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's			
CC6.5.1	Media handling and disposal procedures are in place to guide	Inspected StrongestLayer, Inc.'s data management policy to determine that	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	personnel in performing sanitization procedures on all accounts where production data resides so that data and software are unrecoverable prior to retiring the asset.	media handling and disposal procedures are in place to guide personnel in performing sanitization procedures on all accounts where production data resides so that data and software are unrecoverable prior to retiring the asset.	
CC6.5.2	Electronic media containing confidential information are purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	1. Obtained a population of media disposals across the entire audit period and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the electronic media containing confidential information are purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no media or device disposal occurred during the review period.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The Company perimeter protection systems are configured to deny unauthorized traffic from external sources and do not provide special access privileges to those outside of its hosted project.	Inspected StrongestLayer, Inc.'s Firewall to determine that the perimeter protection systems are configured to deny unauthorized traffic from external sources and do not provide special access privileges to those outside of its hosted project.	No exceptions noted.
CC6.6.2	Web servers use TLS encryption for web communication sessions.	Inspected StrongestLayer, Inc.'s Encryption to determine that web servers use TLS encryption for web communication sessions.	No exceptions noted.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Encryption technologies such as VPN, TLS, and SFTP are used to protect communications and data during transmission.	Inspected StrongestLayer, Inc.'s Encryption to determine that encryption technologies such as VPN, TLS, and SFTP are used to protect communications and data during transmission.	No exceptions noted.
CC6.7.2	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company utilizes anti-malware software that is centrally managed and deployed on client machines and is monitored for unauthorized or malicious software installations.	Inspected StrongestLayer, Inc.'s Anti-Malware Protection to determine that it utilizes anti-malware software that is centrally managed and deployed on client machines and is monitored for	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
		unauthorized or malicious software installations.	
CC6.8.2	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The Company performs network vulnerability scans on at least an annual basis and remediates critical vulnerabilities identified in a timely manner.	Inspected StrongestLayer, Inc.'s scan results and ongoing remediation to determine that vulnerability scans were performed at least annually to identify security issues and were remediated in a timely.	No exceptions noted.
CC7.1.2	Annual penetration testing is conducted by an independent third party on the network and on the Platform application.	Inspected StrongestLayer, Inc.'s annual penetration testing to determine if it was conducted by an independent third party on the network and on the Platform application.	No exceptions noted.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	An Intrusion Detection System (or equivalent) is in place to alert personnel to unauthorized modifications of critical system files, configuration files, and content files.	Inspected StrongestLayer, Inc.'s infrastructure monitoring configurations and monitoring rulesets to determine that an Intrusion Detection System (or equivalent) is in place to alert personnel to unauthorized modifications of critical system files, configuration files, and content files.	No exceptions noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	IT Operations personnel review identified security events to determine impact and to recommend remediation, if necessary.	Inspected StrongestLayer, Inc.'s security event tickets to determine that IT Operations personnel review identified security events to determine impact and to recommend remediation, if necessary.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security events occurred during the review period.
CC7.3.2	The company has incident response policies and processes documented to handle security and/or data breach incidents.	Inspected StrongestLayer, Inc.'s Incident Response Policy to determine that the company has policies and processes documented to handle security and/or data breach incidents.	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company has incident response policies and processes documented to handle security and/or data breach incidents.	Inspected StrongestLayer, Inc.'s Incident Response Policy to determine that the company has policies and processes documented to handle security and/or data breach incidents.	No exceptions noted.
CC7.4.2	Security and privacy incidents, including instances of noncompliance, are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the security incident tickets to determine that security and privacy incidents, including instances of noncompliance, are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has recovery plans in place to provide processes for recovery systems as needed after incidents or other types of outages.	Inspected StrongestLayer, Inc.'s Business Continuity Planning and Disaster Recovery Policy to determine that the company has recovery plans in place to provide processes for recovery systems as needed after incidents or other types of outages.	No exceptions noted.
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change requests are submitted via a Change Request form and are entered into a ticket system for tracking. Management approval is obtained and documented in each change ticket.	1. Obtained a population of access changes across the entire audit period and selected a sample according to our sampling guidance. 2. For the samples selected, inspected the change tickets to determine that change requests are submitted via a Change Request form and are entered into a ticket system for tracking. Management approval is obtained and documented in the selected change tickets.	No exceptions noted.
CC8.1.2	The Platform application development and testing are done in separate environments from production.	Inspected the production and development environment configurations to determine that the system application development and testing are done in separate environments from production.	No exceptions noted.
CC8.1.3	Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes. The policies and	Inspected StrongestLayer, Inc.'s Change Management / SDLC Policy & Procedure to determine that policies and procedures are in place to guide personnel in the request,	No exceptions noted.

Trust Services Criteria	Description of StrongestLayer, Inc.'s Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	procedures also outline the requirement for segregation of duties such that authorization, development, testing, and implementation are segmented functions within the process.	documentation, testing, and approval of changes. The policies and procedures also outline the requirement for segregation of duties such that authorization, development, testing, and implementation are segmented functions within the process.	
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The Company has developed a written business continuity plan and disaster recovery plan with procedures to protect against disruptions caused by an unexpected event.	Inspected StrongestLayer, Inc.'s Business Continuity Planning and Disaster Recovery Policy to determine that the company has developed a written business continuity plan and disaster recovery plan with procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The Company management reviews the Annual SOC 2 report (or equivalent) for its hosted data center to confirm that outsourced controls are appropriately designed and operating effectively.	Inspected StrongestLayer, Inc.'s SOC 2 report and review to determine that the management reviews the annual SOC report for its hosted data center to confirm that outsourced controls are appropriately designed and operating effectively.	No exceptions noted.
CC9.2.2	A vendor management process is in place and requires a signed contract for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	Inspected StrongestLayer, Inc.'s Vendor Review to determine that a vendor management process is in place and requires a signed contract for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	No exceptions noted.