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


wvOASIS
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Header
List View
General Information
Contact
Default Values
Discount
Document Information
Certification Request
Procurement Folder:
Procurement Type: Central Contract - Fixed Amt
Vendor ID:
Legal Name: Tailored Solutions and Consulting
Alias/DBA: Secure Halo
Total Bid:
Response Date:
Response Time:
Responded By User ID:
First Name: Ryan
Last Name:
Email:
Phone:
SO Doc Code: CRFQ
SO Dept:
SO Doc ID:
Published Date:
Close Date:
Close Time:
Status: Closed
Solicitation Description: Addendum No 1 Cybersecurity/ Privacy Training
Total of Header Attachments: 1
Total of All Attachments: 1

**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:** | 1619671 |
| **Solicitation Description:** | Addendum No 1 Cybersecurity/ Privacy Training (OT25069) |
| **Proc Type:** | Central Contract - Fixed Amt |

| Solicitation Closes | Solicitation Response | Version |
|---|---|---|
| 2025-02-25 13:30 | SR 0231 ESR02252500000005196 | 1 |

**VENDOR**

VS0000048340
Tailored Solutions and Consulting

**Solicitation Number:** CRFQ 0231 OOT2500000016

**Total Bid:** 290000 **Response Date:** 2025-02-25 **Response Time:** 09:19:11

**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 | Privacy and Cybersecurity Training Solution | 1.00000 | YR | 72500.000000 | 72500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Commodity Line Comments:**

**Extended Description:**

Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 2 | Privacy and Cybersecurity Training Solution-Optional YR2 | 1.00000 | YR | 72500.000000 | 72500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Commodity Line Comments:**

**Extended Description:**

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 3 | Privacy and Cybersecurity Training Solution-Optional YR3 | 1.00000 | YR | 72500.000000 | 72500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Commodity Line Comments:**

**Extended Description:**

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 4 | Privacy and Cybersecurity Training Solution-Optional YR4 | 1.00000 | YR | 72500.000000 | 72500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Commodity Line Comments:**

**Extended Description:**

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

CRFQ OOT2500000016

# Cybersecurity/Privacy Training

*February 25, 2025*

**State of West Virginia**

SECURE HALO
SECURING THE ENTERPRISE
A **Mission Critical Partners** Company

# Table of Contents


Introduction Letter ..... 1
About Secure Halo ..... 2
General Requirements ..... 3
Cybersecurity Training Services ..... 3
- Phishing Simulation Exercises ..... 3
- Security Training ..... 4
- Sample Proposed Timeline ..... 4
- Implementation ..... 4
- Frequency ..... 5
- Updates ..... 5

Evaluation and Reporting ..... 6
- Assessment Tools ..... 6
- Key Performance Indicators (KPIs) ..... 6
- Security Practices ..... 6

Pricing ..... 7
References ..... 8
Required Forms ..... 8

# Introduction Letter

February 25, 2025

State of West Virginia, Department of Administration

Purchasing Division

2019 Washington Street East

Post Office Box 50130

Charleston, West Virginia 25305-0130

CRFQ OOT2500000016 – Cybersecurity/Privacy Training

Dear State of West Virginia Department of Administration, Purchasing Division:

Secure Halo is pleased to provide this Cybersecurity Training proposal to The State of West Virginia in support of training users of their network on common technical cyber-attack tactics.

By the signature of Secure Halo's authorized representative hereunder, this project proposal constitutes Secure Halo's formal offer to provide the services and/or deliverables on the terms and conditions described herein.

This project proposal will be valid for a period of 30 days.

On behalf of our entire team, we stand behind The State of West Virginia to serve as your partner and your advocate.

Sincerely,

Secure Halo, a Mission Critical Partners company

Matthew Yates
Secure Halo

Director, Operations

# About Secure Halo


Secure Halo™, a Mission Critical Partners company, has more than a decade of experience supporting the business community and federal agencies with their cybersecurity needs. We provide highly specialized solutions to a host of clients, ranging from large, complex organizations across the Fortune 500, to leading insurance underwriting markets, U.S. critical infrastructure, healthcare, and financial services. Our solutions have been leveraged by the federal government to guide and shape policy across the critical infrastructure, telecommunications, and IT infrastructure domains to ensure a resiliency within the U.S. enterprise.

Secure Halo is an innovative leader in cybersecurity and risk management, risk assessments, cybersecurity assessments, pen tests, and remediation services. We also have extensive experience in areas such as information assurance, insider threats, corporate espionage, and data analytics.

We work alongside clients as trusted advisors, keeping client confidentiality paramount. We thoroughly examine enterprise risk from a holistic perspective. Our unique approach maximizes clients' returns on security investments by delivering objective and practical solutions designed to "Find, Fix, Protect" critical areas.

Secure Halo became part of Mission Critical Partners (MCP) in 2022. MCP is a leading provider of data integration, consulting, network, and cybersecurity services. Our vision is to transform mission-critical and public-sector networks and operations into integrated and secure ecosystems.

## Benefits of selecting Secure Halo for this project:

- Delivery of cost-effective training solutions
- Extraordinary track record of improving client workflow and efficiencies
- Deep domain knowledge and expertise in cybersecurity and offensive cyber strategies and solutions

BECAUSE
THE MISSION
MATTERS

SECURE HALO
SECURING THE ENTERPRISE
A Mission Critical Partners Company

# General Requirements

It is our understanding that The State of West Virginia is in need of training services for the users of their networks to help identify and mitigate the risks of common cyber-attack tactics. The project goal is to help the staff, end users and any other supporting or contracting staff have access to materials that will help enhance awareness of cybersecurity risks, identifying potential attacks and understanding cybersecurity best practices.

Secure Halo has been a leader in cybersecurity for 20 years and has worked with 400+ K-12 school districts, Fortune 500 companies and Critical Infrastructure in assessment, training and remediation. Secure Halo has also been intimately involved in the creation of cyber risk policies in the insurance industry, helping companies understand the true cost and impact of cyber-attacks on an organization. It is our goal to use that wealth of experience to help tailor a training program to The State of West Virginia's specific needs, including but not limited to: insurance requirements, any applicable federal, state or local laws, industry standards and to mitigate risks from phishing, ransomware and other common technical attacks.

# Cybersecurity Training Services

Training and assessing enterprises' cyber awareness and readiness is not a one-size-fits-all endeavor. Each industry and organization present unique challenges that must be understood to properly and effectively deliver training solutions. It is with that in mind that Secure Halo has created the following training plan for The State of West Virginia.

## Phishing Simulation Exercises

Secure Halo will conduct customized phishing exercises that are designed to test employee's ability to recognize and report suspicious emails.

1) Secure Halo will conduct monthly (12) simulated phishing email campaigns on all employees of each location member of The State of West Virginia. Secure Halo will proactively coordinate with each location to collect mailing lists, schedule the phishing tests, and work with internal IT staff to ensure emails get through any filters to truly test employee awareness. Secure Halo will coordinate with each location member to ensure efficient and collaborated delivery of phishing exercises which will follow the standard steps below:
   a) IT Staff send updated employee email list to Secure Halo
   b) Secure Halo delivers whitelist instructions to ensure emails arrive directly in employee inboxes.
   c) IT Staff implement whitelist instructions.
   d) Secure Halo sends test email to confirm successful receipt.
   e) IT Staff replies with confirmation and screenshot.
   f) Secure Halo schedules and executes phishing email exercise.
   g) Secure Halo delivers report detailing results from the exercise.

2) Secure Halo will initiate remedial training for employees who either click the phishing links or submit data to the phishing site. Training is web-based and will require the employees to take, and pass, a quiz at the end to ensure employees are gaining awareness from the training.

3) Secure Halo will deliver a Phishing Test Results Report that details:

a) Avoided/Opened/Clicked Statistics
b) List of employees who clicked phishing links or submitted data.
c) Phishing Timeline

## Security Training

Secure Halo will provide training resources for all employees in order to help educate and advance cybersecurity awareness within The State of West Virginia. Secure Halo has a platform with over 200 training courses and material to choose from. We also offer the ability to create customized training courses specific to the client's needs.

1) Secure Halo will conduct monthly (12) training and awareness campaigns delivered via email to all employees of each location of The State of West Virginia. Secure Halo will utilize the mailing list for the monthly phishing campaigns as the list for the training and awareness campaigns. Topics for the Security Trainings and Awareness will be selected at time of contract signature. Secure Halo can add the following to the training courses for The State of West Virginia:

   a) The State of West Virginia logo and custom training URL
   b) Quizzes at the end of each training
   c) Number of Quiz attempts
   d) Passing percentage for Quizzes (i.e. 70%)

## Sample Proposed Timeline

| Service | Freq | Feb | Mar | Apr | May | June | Jul | Aug | Sep | Oct | Nov | Dec | Jan |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phishing Exercises | Monthly (12) | | | | | | | | | | | | |
| Security Trainings | Monthly (12) | | | | | | | | | | | | |

## Implementation

**Initial Setup and Deployment Timeline**

**Phase 1: Planning & Setup (Month 1-2)**

- Conduct kickoff meeting with The State of West Virginia to align expectations.
- Gather staff directory for phishing and training campaign targeting.

- Develop customized training content incorporating district policies, regulatory requirements (FERPA, CIPA, COPPA, HIPAA), and best practices.
- Configure training platform for access, reporting, and tracking.
- Schedule training campaigns and phishing exercises.

**Phase 2: Pilot Testing (Month 3)**

- Run initial phishing exercise to gauge awareness baseline.
- Conduct first security training session.
- Evaluate results and gather feedback for refinement.

**Phase 3: Full Rollout (Month 4 and Beyond)**

- Initiate monthly phishing simulations.
- Conduct monthly security training campaigns.

## Frequency

**Training & Assessment Frequency**

| Service | Frequency |
|---|---|
| Phishing Exercises | Monthly (12 per year) |
| Security Trainings | Monthly (12 per year) |

## Updates

**Regulatory Compliance & Threat Landscape Updates**

- Training materials reviewed quarterly to integrate emerging threats.
- Updates aligned with FERPA, CIPA, COPPA, HIPAA, and Colorado HB 21-1110 accessibility standards.
- Adapt training to reflect changes in NIST CSF, ISO 27001, and CIS Critical Security Controls.

**Employee Awareness & Engagement Enhancements**

- Quarterly reports on phishing test results and remedial training.
- Live Q&A sessions during security webinars.
- Interactive quizzes with updated scenarios in training sessions.
- Customizable content to address specific concerns.

# Evaluation and Reporting

## Assessment Tools

Regular phishing exercises will test the effectiveness of the training over time and gauge staff awareness and response. This will be supplemented by security training courses and security webinars on relevant topics. Over the course of the required training, employees will become more aware and engaged in proactive cybersecurity mitigation as well as recognizing potential cybersecurity threats.

## Key Performance Indicators (KPIs)

Our phishing simulation exercises provide metrics on how many users engaged with the simulated phishing attack. This includes opened, clicked and whether the user entered data. Security trainings provide engagement and scores for users.

## Security Practices

Our organization is committed to maintaining the highest standards of security, privacy, and compliance to protect sensitive data and ensure the integrity of our services. We implement industry-leading security controls to safeguard information against cyber threats, unauthorized access, and data breaches.

Key Security Commitments

1. **Data Protection** – All data is encrypted in transit and at rest, ensuring confidentiality and integrity.
2. **Access Control** – Role-based access, multi-factor authentication (MFA), and least privilege principles are enforced.
3. **Compliance & Standards** – Our security framework aligns with NIST, ISO 27001, CIS Controls, and regulatory mandates such as FERPA, CIPA, COPPA, and HIPAA.
4. **Secure Development & Patching** – Regular updates, vulnerability assessments, and penetration testing ensure proactive risk mitigation.
5. **Data Privacy & Governance –** Adhering to strict data retention and disposal policies, we comply with NIST 800-88 and other best practices to safeguard information.
6. **Security Awareness & Training –** Ongoing employee cybersecurity training, phishing simulations, and compliance updates reinforce a culture of security.

By integrating robust security controls, continuous improvement, and regulatory compliance, we ensure the protection, availability, and reliability of our services.

# Pricing

| Service | Year 1 | Year 2 | Year 3 | Year 4 |
|---|---|---|---|---|
| **Phishing Exercises** | $37,500.00 | $37,500.00 | $37,500.00 | $37,500.00 |
| **Security Trainings** | $35,000.00 | $35,000.00 | $35,000.00 | $35,000.00 |
| **Lump Sum** | **$72,500.00** | **$72,500.00** | **$72,500.00** | **$72,500.00** |

# References

**Weld RE-4 School District**

1020 Main Street

Windsor, Colorado 80550

Stephen Gagliardi, Enterprise Technology Manager

Stephen.gagliardi@weldre4.org

Description of effort: Currently engaged in a NIST 2.0 Risk Assessment, Internal and External Vulnerability Assessment, Governance and Compliance Consulting and Incident Response Consulting.

**Arthur J, Gallagher & Co.**

2 Stevenson Drive

Lincolnshire, Illinois 600069

Dr. Sean Carney, Chairman

scarney@d125.org

Description of effort: Currently engaged in Best Practices Assessment for several Insurance Pools of 400+ schools. Consortium is used to reduce insurance costs and better provide services to member districts.

**Township District 113**

1040 Park Avenue

West Highland Park, Illinois 60065

Ron Kasbohm, Chief Information Officer

rkasbohm@dist113.org

Description of effort: Internal and External Penetration Test, Web Application Test, Social Engineering Test, Wireless Network Test, Ransomware Simulation, Documentation Review and Consulting.

**Piqua City Schools**

215 Looney Road

Piqua, Ohio 45356

Erich Heidenreich, Director of Technology

erich@piqua.org

Description of effort: Multi-year Phishing Simulation, Security Training and Darkweb Monitoring subscription.

# Required Forms

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:** 1619671<br>**Doc Description:** Cybersecurity/ Privacy Training (OT25069)<br>**Proc Type:** Central Contract - Fixed Amt | | | **Reason for Modification:** |
| **Date Issued** | **Solicitation Closes** | **Solicitation No** | **Version** |
| 2025-02-06 | 2025-02-25 13:30 | CRFQ 0231 OOT2500000016 | 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 :** Tailored Solutions and Consulting dba Secure Halo

**Address :** Suite 310

**Street :** 962 Wayne Ave

**City :** Silver Spring

**State :** MD **Country :** USA **Zip :** 20910

**Principal Contact :** Ryan Krug

**Vendor Contact Phone:** 202-240-1938 **Extension:**

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

**Vendor Signature X** Ryan Krug **FEIN#** 45-3968550 **DATE** 02/25/2025

**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 a contract for the purchase of customized Cybersecurity and Privacy Training that is hosted in a vendor-managed Learning Management System (LMS). The WVOT is seeking a product that will provide security and privacy training for an estimated 25,000 end users with an integrated phishing simulator and training per the terms and conditions and specifications as attached. |

| 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 | Privacy and Cybersecurity Training Solution | 1.00000 | YR | $72,500.00 | $72,500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Extended Description:**
Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

| 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 | Privacy and Cybersecurity Training Solution-Optional YR2 | 1.00000 | YR | $72,500.00 | $72,500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Extended Description:**
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

| 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 | Privacy and Cybersecurity Training Solution-Optional YR3 | 1.00000 | YR | $72,500.00 | $72,500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Extended Description:**
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

| 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 | Privacy and Cybersecurity Training Solution-Optional YR4 | 1.00000 | YR | $72,500.00 | $72,500.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 43232502 | | | |

**Extended Description:**
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Questions are due by 3:00 p.m. | 2025-02-14 |

| | Document Phase | Document Description | Page<br>4 |
|---|---|---|---|
| OOT2500000016 | Draft | Cybersecurity/ Privacy Training ( OT25069) | |

**ADDITIONAL TERMS AND CONDITIONS**

See attached document(s) for additional Terms and Conditions

**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) Ryan Krug, Senior Business Operations Analyst

(Address) 962 Wayne Ave Suite 310, Silver Spring, MD 20910

(Phone Number) / (Fax Number) 202-240-1938

(email address) rkrug@securehalo.com

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

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

Tailored Solutions and Consulting dba Secure Halo
(Company)

Ryan Krug
(Signature of Authorized Representative)

Ryan Krug, Senior Business Operations Analyst 02/25/2025
(Printed Name and Title of Authorized Representative) (Date)

202-240-1938
(Phone Number) (Fax Number)

rkrug@securehalo.com
(Email Address)

**ADDENDUM ACKNOWLEDGEMENT FORM**
**SOLICITATION NO.:** CRFQ OOT25*016

**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.

Tailored Solutions and Consulting dba Secure Halo
Company

Ryan Krug
Authorized Signature

02/25/2025
Date

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