SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.

2. CONTRACT NO.

3. AWARD/EFFECTIVE DATE

4. ORDER NO.

5. SOLICITATION NUMBER: 36C10B26Q0396

6. SOLICITATION ISSUE DATE: 06-25-26

7. FOR SOLICITATION INFORMATION CALL:
a. NAME: Allison Fulton, Allison.Fulton@va.gov
b. TELEPHONE NO. (No Collect Calls): 848-377-5512

8. OFFER DUE DATE/LOCAL TIME: 07-07-2026 11:00 AM CDT

9. ISSUED BY — CODE 36C10B
Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

10. THIS ACQUISITION IS
[X] UNRESTRICTED OR [ ] SET ASIDE: ____ % FOR:
[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
[ ] EDWOSB
[ ] 8(A)

NAICS: 541519

SIZE STANDARD: 150 Emp

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING: N/A

14. METHOD OF SOLICITATION
[X] RFQ [ ] IFB [ ] RFP

15. DELIVER TO — CODE
See instructions in Product Description

16. ADMINISTERED BY — CODE 36C10B
Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

17a. CONTRACTOR/OFFEROR — CODE — FACILITY CODE

TELEPHONE NO. — UEI: — EFT:

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE 36C10A
Department of Veterans Affairs
Technology Acquisition Center
Financial Services Center
PO Box 149971
Austin TX 78714-8971

PHONE: (877) 353-9791 FAX:

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
[ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Title: Orlando Veterans Affairs Healthcare System (OVAHCS) Employee Recognition Platform and Service Period of Performance (PoP): 12-month base period, with four 12-month option periods. ***See continuation pages*** Points of Contact (POC): Contracting Officer: Mina Awad, Mina.Awad@va.gov Contract Specialist: Allison Fulton, Allison.fulton@va.gov				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA
See Continuation Page

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED.

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT): Mina Awad

31c. DATE SIGNED

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS 3

B.1 GOVERNING LAW CLAUSE 3
B.2 SOFTWARE LICENSE, SOFTWARE MAINTENANCE, AND SOFTWARE TECHNICAL SUPPORT 4
B.3 CONTRACT ADMINISTRATION DATA 9
B.4 PRICE SCHEDULE 10
B.5 PRODUCT DESCRIPTION 12

SECTION C - CONTRACT CLAUSES 43

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 43
C.2 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JUN 2020) 44
C.3 52.209-6 Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded 47
C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 48
C.5 52.219-8 UTILIZATION OF SMALL BUSINESS CONCERNS 48
C.6 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026) 52
C.7 852.211-76 LIQUIDATED DAMAGES – REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023) ALTERNATE I (FEB 2023) 53
C.8 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY 54

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 56

SECTION E - SOLICITATION PROVISIONS 57

E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) 57
E.2 FAR 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (NOV 2025 (DEVIATION)) 58
E.3 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (NOV 2025) 59
E.4 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (FEB 2016) 61
E.5 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION) 61
E.6 52.233-2 SERVICE PROTEST (NOV 2025) 61
E.7 BASIS FOR AWARD 62
E.8 QUOTE SUBMISSION INSTRUCTIONS 62

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW CLAUSE

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (*e.g.*, restricted computer software) are included and made a part of this Contract/Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 *et seq*.), the Anti-Deficiency Act (31 U.S.C. § 1341 *et seq*.), the Competition in Contracting Act (41 U.S.C. § 3301 *et seq*.), the Prompt Payment Act (31 U.S.C. § 3901 *et seq*.), Contracts for Data Processing or Maintenance (38 USC § 5725), Source Code Harmonization and Reuse in Information Technology Act "SHARE IT Act" (P.L. 118-187), and FAR clauses 52.212-4, 52.227-14 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, this includes any custom code developed for the purpose of performing under this contract. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ) in accordance with 28 U.S.C. § 516; at the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by modification (Standard Form 30) and shall only be made by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.2 SOFTWARE LICENSE, SOFTWARE MAINTENANCE, AND SOFTWARE TECHNICAL SUPPORT

(1). **Definitions.**

a) Licensee. The term "licensee" shall mean the U.S. Department of Veterans Affairs ("VA") and is synonymous with "Government."

b) Licensor. The term "licensor" shall mean the Contractor having the necessary license or ownership rights to deliver license, software maintenance and support of the computer software being acquired. The term "Contractor" is the party identified in Block 17a on the SF1449. If the Contractor is a reseller and not the Licensor, the Contractor remains responsible for performance under this Contract/Order.

c) *Software.* The term "software" shall mean the licensed computer software product(s) cited in the Schedule of Supplies/Services.

d) *Maintenance.* The term "maintenance" is the process of enhancing and optimizing software, as well as remedying defects. It shall include all new fixes, patches, releases, updates, versions and upgrades, as further defined below.

e) *Technical Support.* The term "technical support" refers to the range of services providing assistance for the software via the telephone, email, a website or otherwise.

f) *Release or Update.* The term "release" or "update" are terms that refer to a revision of software that contains defect corrections, minor enhancements, or improvements of the software's functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.

g) *Version or Upgrade.* The term "version" or "upgrade" are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

(2). **Software License.**

a) Unless otherwise stated in the Schedule of Supplies/Services, the Performance Work Statement, or Product Description, the software license provided to the Government is a perpetual, nonexclusive license to use the software.

b) The Government may use the software in a networked environment.

c) All limitations of software usage are expressly stated in the Schedule of Supplies/Services and the Performance Work Statement/Product Description.

d) The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided below or as expressly stated otherwise in this contract. The

commercial computer software may be-

i. Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation or agency to which the computer(s) may be transferred;
ii. Used or copied for use with a backup computer if any computer for which it was acquired is inoperative;
iii. Reproduced for safekeeping (archives) or backup purposes;
iv. Modified, adapted, or combined with other computer software;
v. Disclosed to and reproduced for use by support service Contractors or their subcontractors, subject to the same restrictions set forth in this contract; and
vi. Used or copied for use with a replacement computer.

e) Unauthorized Obligations.
   i. Except as stated in paragraph (ii), when any supply or service acquired under this contract is subject to any commercial supplier agreement (as defined in 502.101) that includes any language, provision, or clause requiring the Government to pay any future fees, penalties, interest, legal costs or to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:
      1) Any such language, provision, or clause is unenforceable against the Government.
      2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.
      3) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement.
   ii. Paragraph (u)(1) of this clause does not apply to indemnification or any other payment by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

f) Commercial supplier agreements unenforceable clauses.
   i. This agreement is a part of a contract between the commercial supplier and the U.S. Government for the

acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR 12).

ii. *End user.* This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.

iii. *Law and disputes*. This agreement is governed by Federal law. Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted.

1) Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted. Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).
2) Any language prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.
3) *Continued performance*. The supplier or licensor shall not unilaterally revoke, terminate or suspend any rights granted to the Government except as allowed by this contract. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing.
4) *Arbitration; equitable or injunctive relief*. In the event of a claim or dispute arising under or relating to this agreement, a binding arbitration shall not be used unless specifically authorized by agency guidance, and equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).

iv. *Updating terms*. After award, the contractor may unilaterally revise commercial supplier agreement terms if they are not material. A material change is defined as:

1) Terms that change Government rights or obligations;
2) Terms that increase Government prices;
3) Terms that decrease overall level of service; or
4) Terms that limit any other Government right addressed elsewhere in this contract.
5) For revisions that will materially change the terms of

the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.

6) Any agreement license terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provision of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

v. *No automatic renewals*. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by an authorized Government representative.

vi. *Indemnification*. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

vii. *Audits*. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user's compliance with this agreement is hereby amended as follows:

1) Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order.
2) This charge, if disputed by the ordering activity, will be resolved in accordance with FAR 52.212-4(d); no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process.
3) Any audit requested by the contractor will be performed at the contractor's expense, without reimbursement by the Government.

(3). Software Maintenance and/or Technical Support.

a) If the Government desires to continue software maintenance and support beyond the period of performance identified in this Contract/Order, the Government will issue a separate contract or order for maintenance and support. Conversely, if a contract or order for continuing software maintenance and technical support is not received, the Contractor is neither authorized nor permitted to renew any of the previously furnished services.
b) The Contractor shall provide software support services, which includes periodic updates, enhancements and corrections to the

software, and reasonable technical support, all of which are customarily provided by the Contractor to its commercial customers to cause the software to perform according to its specifications, documentation or demonstrated claims.

c) Any telephone support provided by Contractor shall be at no additional cost.

d) The Contractor shall provide all maintenance services in a timely manner in accordance with the Contractor's customary practice or as defined in the Performance Work Statement or Product Description. However, prolonged delay (exceeding two business days) in resolving software problems will be noted in the Government's various past performance records on the Contractor (e.g., www.cpars.gov).

e) If the Government allows the maintenance and support to lapse and subsequently wishes to reinstate it, any reinstatement fee charged shall not exceed the amounts that would have been charged if the Government had not allowed the subscription to lapse.

(4). Disabling Software Code.

The Government requires delivery of computer software that does not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable the software. Such code includes but is not limited to a computer virus, restrictive key, node lock, time-out, or other function, whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration of use, or other limiting criteria. If any such disabling code is present, the Contractor agrees to indemnify the Government for all damages suffered as a result of a disabling caused by such code, and the contractor agrees to remove such code upon the Government's request at no extra cost to the Government. Inability of the Contractor to remove the disabling software code will be considered an inexcusable delay and a material breach of contract, and the Government may exercise its right to terminate for cause. In addition, the Government is permitted to remove the code as it deems appropriate and charge the Contractor for consideration for the time and effort expended in removing the code.

(5). Manuals and Publications.

Upon Government request, the Contractor shall furnish the most current version of the user manual and publications for all products/services provided under this Contract/Order at no cost.

B.3 CONTRACT ADMINISTRATION DATA

1. Contract Administration: All contract administration matters will be handled by the following individuals:

   a. CONTRACTOR: To Be Determined (TBD)

   b. GOVERNMENT: Contracting Officer 36C10B
   Department of Veterans Affairs
   Technology Acquisition Center
   23 Christopher Way
   Eatontown NJ 07724

   c. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

[X] 52.232-33, Payment by Electronic Funds Transfer—System For Award Management, or

[] 52.232-36, Payment by Third Party

   d. INVOICES: Invoices shall be submitted in arrears:

a. Quarterly []
b. Semi-Annually []
c. Other [X] Upon acceptance of Deliverables in accordance with Section B.4, Price Schedule

   e. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

   f. ACKNOWLEDGMENT OF AMENDMENTS: The offeror acknowledges receipt of amendments to the Solicitation numbered and dated as follows:

AMENDMENT NO	DATE

B.4 PRICE SCHEDULE

NOTE: Vendors are instructed to complete Section B.4 and submit with their quote.

Offerors are cautioned that alterations to the line items as specified below may render quotes unacceptable. All questions shall be directed to the Contract Specialist, Allison Fulton, Allison.Fulton@va.gov, prior to the closing date and time specified in the Request for Quote (RFQ).

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Base Period **The Period of Performance (PoP) shall be 12 months from the date of award.**					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Total Price**
0001	Annual Platform, Configuration and Training Fee – Base PSC: 7A21	1	LOT (LO)	$	$
0001AA	Compliance Monitoring and Reporting Plan Due within 30 days after contract award	1	LO	NSP	NSP
0001AB	Corrective Action Plan Due within 30 days after contract award	1	LO	NSP	NSP
0001AC	AI Model/LLM Change Disclosure Due within 30 days after contract award	1	LO	NSP	NSP
Base Period Total:				**$**	
Option Period One **This Option Period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract. Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer (CO). If exercised, this option shall commence immediately after expiration of the Base Period.**					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Total Price**
1001	Option Year (OY 1) Subscription Fee (includes Technical Support as needed) PSC: 7A21	1	LO	$	$
Option Period One Total:				**$**	
Option Period Two **This Option Period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract. Work shall not commence until, and unless, a formal modification is issued by the CO. If exercised, this option shall commence immediately after expiration of Option Period One.**					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Total Price**
2001	OY 2 Subscription Fee (includes Technical Support as needed) PSC: 7A21	1	LO	$	$
Option Period Two Total:				**$**	

Option Period Three This Option Period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract. Work shall not commence until, and unless, a formal modification is issued by the CO. If exercised, this option shall commence immediately after expiration of Option Period Two.					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Total Price**
3001	OY 3 Subscription Fee (includes Technical Support as needed) PSC: 7A21	1	LO	$	$
Option Period Three Total:				**$**	

Option Period Four This Option Period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract. Work shall not commence until, and unless, a formal modification is issued by the CO. If exercised, this option shall commence immediately after expiration of Option Period Three.					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Total Price**
4001	OY 4 Subscription Fee (includes Technical Support as needed) PSC: 7A21	1	LO	$	$
Option Period Four Total:				**$**	
TOTAL ORDER VALUE (INCLUSIVE OF ALL OPTION PERIODS):				**$**	

B.5 PRODUCT DESCRIPTION

PRODUCT DESCRIPTION (PD)
DEPARTMENT OF VETERANS AFFAIRS

Veterans Health Administration (VHA)
Orlando Veterans Affairs Healthcare System (OVAHCS)

OVAHCS Employee Recognition Platform and Service

Date: May 1, 2026
VA-26-00052104
PD Version Number: 1.0

1.0 PRODUCT REQUIREMENTS

The Department of Veterans Affairs (VA), OVAHCS, has a requirement to provide a Healthcare driven digital, cloud-based employee recognition platform that enables employees, patients, caregivers, and family members to recognize OVAHCS clinical and non-clinical staff for exemplary customer care and support.

The platform shall utilize a push/pull technology approach to healthcare employee recognition by facilitating real-time feedback from patients, peers, caregivers, and family members (pull), and by delivering personalized recognition and actionable data to staff (push).

The platform shall include, at a minimum, the capability to:

- Generate detailed reports measuring patient satisfaction, patient safety, and staff recognition data.
- Capture real-time, in-the-moment patient feedback.
- Provide prioritized, real-time results and insights.
- Offer marketing and communication tools that support efforts to improve patient experience and employee engagement.

The platform shall support unlimited data pulls by the organization and must accommodate at least 6,648 OVAHCS employees. The Contractor shall provide technical support services sufficient to ensure full and continuous functionality of the platform for all covered users.

1.1 SALIENT CHARACTERISTICS

1. Allow Veterans and family members to digitally recognize staff members who positively impact their care journey.
2. Provide an easy-to-use, real-time interface that allows Veterans and families to submit recognition directly from mobile devices or digital access points during their visit.
3. Enable Veterans to recognize individuals who impacted their experience across clinical and non-clinical roles.
4. Support at a minimum number of two languages to include English and Spanish to ensure accessibility for diverse populations.
5. Deliver positive Veteran feedback directly to staff members through a platform accessible to their peers and leadership. While screening and redacting any protected health information (PHI) in compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements.
6. Enable real-time service recovery opportunities by privately routing any constructive feedback to relevant leaders.
7. Integrate existing recognition programs (e.g., Diseases Attacking the Immune System (DAISY) Award nominations) into a unified workflow, enabling Veterans and family members to submit nominations directly through the interface.

8. Ask configurable questions related to a Veteran's experience with specific staff members and provide individualized Veteran experience insights to employees and leadership.
9. Enable real-time notifications to staff and leaders when recognition is received.
10. Provide resources to support marketing to promote awareness and adoption of the healthcare patient driven recognition program.
11. Ensure healthcare workers receive meaningful and frequent recognition by incorporating the voice of leaders, peers, Veterans, and their families.
12. Reinforce Integrity, Commitment, Advocacy, Respect, and Excellence (ICARE) values by incentivizing and promoting mission-aligned behaviors across staff.
13. Provide team recognition capabilities to include: Veteran-to-staff, peer-to-peer, leader-to-staff, and leader-to-team.
14. Enhance employee engagement by highlighting the impact of staff contributions through healthcare patient driven recognition.
15. Support employee celebrations including service anniversaries, new hires, milestones, and other culture-building events.
16. Provide an internal social engagement environment that allows patient-driven stories, positive experiences, and communication to be shared between individuals, teams, groups, departments, and across the organization.
17. Enable leadership to communicate organizational priorities through digital communication tools within the platform.
18. Provide opportunities to highlight positive care experiences across departments and service lines.
19. Provide interactive challenges that promote teamwork, patient experience, quality, safety, and positive workplace behaviors.
20. Provide platform user interface design with branding customization and data insights to drive organization improvements
21. Provide real-time reporting and analytics to identify trends related to Veteran experience, staff engagement, and recognition activity.
22. Deliver platform insights directly to leaders to surface areas of strength and share opportunities on how to make the biggest impact on your team
23. Support data access and reporting capabilities to inform leadership decision making.
24. Provide Software-as-a-Service based interactive software hosted in a secure cloud environment.
25. Support access across Android and iOS devices.
26. Include a companion mobile application.
27. Provide Single Sign-On integration with existing authentication and HR systems.
28. Support at least 6,648 users (employees) and provide technical assistance for system issues, connection problems, and application-related errors. Support should also include help desk assistance for patient users.

29. Provide ongoing technical support and system administration services. This includes assisting Admin Client Users with actions such as removing users, updating account information, pausing accounts, and resolving login issues. These functions will be performed by designated onsite Super Users.
30. Require employees with access to sensitive information to sign confidentiality agreements prohibiting unauthorized disclosure of system data
31. Strict control access to restrict private information to privileged users. These users are required to abide by their assigned responsibilities related to their elevated access.
32. Contractor-developed data handling, retention, and disposal processes to manage information in accordance with applicable laws, regulations, policies, and standards. These processes include a formal data retention schedule and a data classification standard designed to ensure the protection and proper handling of confidential data.
33. Retains sensitive and confidential data.
34. Network segmentation to prevent direct or unauthorized connections between an external network and its information systems, in particular confidential data in cloud environments.

Base Period		
Item #	Description	Qty
0001	Annual Platform, Configuration and Training Fee - Base	1

Option Period One		
Item #	Description	Qty
1001	OY 1 Subscription Fee (includes Technical Support as needed)	1

Option Period Two		
Item #	Description	Qty
2001	OY 2 Subscription Fee (includes Technical Support as needed)	1

Option Period Three		
Item #	Description	Qty
3001	OY 3 Subscription Fee (includes Technical Support as needed)	1

Option Period Four		
Item #	Description	Qty
4001	OY 4 Subscription Fee (includes Technical Support as needed)	1

1.2 CONTRACTOR SERVICES

1. The Contractor shall implement an Information Security Management System (ISMS), that adheres to ISO27001 and HIPAA.
2. The Contractor shall be Service Organization Control (SOC) 2 Type II certified.
3. Maintain an information security policy that complies with applicable regulatory and business requirements. This policy must protect all sensitive and confidential data stored, accessed, or transmitted by the software platform, including applications, components, infrastructure, and underlying code.
4. The Contractor shall have a risk assessment program to assess the organization's enterprise-level risk at least annually, or upon significant changes to the environment.
5. The Contractor shall have a comprehensive security awareness training program that is fully implemented. A core set of security training, including HIPAA, for all employees onboarding. The training program also includes monthly updates of latest security threats; annual review of core security training; and team-specific training, as defined by security team.
6. A vulnerability management program to ensure the confidentiality, integrity, and availability (CIA) of the organization's information systems landscape, which includes all critical system resources. The program includes internal and external scans, penetration testing, and issue remediation for the purposes of identifying, detecting, classifying, prioritizing, remediating, validating, and continuously monitoring vulnerabilities.
7. Independent third-party penetration tests at least annually on any systems with Confidential data or with a critical risk rating to identify security vulnerabilities.

1.3 PROJECT MANAGEMENT REQUIREMENTS

1. A project Kick-off call shall be conducted within 14 calendar days of the contract award, as scheduled by OVAHCS and Contractor representatives.
2. Commissioning and operational training shall be done one week from when the platform is fully setup during the hours of 08:00 a.m. – 4:00 p.m. EST Monday- Friday.
3. The Government-recognized US holidays are listed below. If a holiday falls on Sunday, it is observed on Monday.

Holiday	Date	Month
New Year's Day	1st	January
Martin Luther King Jr.'s	3rd Monday	January
President's Day	3rd Monday	February
Memorial Day	Last Monday	May
Juneteenth	19th	June
Independence Day	4th	July
Labor Day	1st Monday	September
Columbus Day	2nd Monday	October
Veterans Day	11th	November
Thanksgiving Day	4th Thursday	November
Christmas Day	25th	December

2.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

2.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with "508 Chapter 2: Scoping Requirements" for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria

- ☐ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

2.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

2.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

If the government determines that Section 508 conformance claims provided by the offeror represent an inaccurate level of conformance than what is actually delivered to the agency, the government shall, at its option, require the offeror to remediate the delivered item to align with the required Section 508 conformance claims prior to acceptance.

3.0 GENERAL REQUIREMENTS

3.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

3.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and

Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

3.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the Integrated Control Number (ICN) in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

3.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 "USGv6 Profile" (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6" (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

3.5 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor's proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

3.6 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative" (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 "Secure External Connections", and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents.)

3.7 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

If Artificial Intelligence (AI) is part of the Contractor system/solution, the Contractor shall be in compliance with E.O. 13960 and 14319, OMB Memorandums M-25-21, M-25-22, and M-26-04, and VA Directive and Handbook 6500 to support VA in trustworthy, secure, responsible, accountable, Truth Seeking, and Ideologically Neutral AI innovation.

No web-based, publicly available generative AI service has been approved for use with VA-sensitive data including, but not limited to OpenAI's ChatGPT, Microsoft's Copilot, Google's Gemini, and Anthropic's Claude. No PII, protected health information (PHI), or VA-sensitive data should be entered into these unapproved services. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23). The Contractor shall protect VA Sensitive data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from VA. Only VA-hosted instances of generative AI services may be approved for use with VA-sensitive data.

The Contractor shall deliver the services, technical data, configurations, models, weights, documentation or other information, including source code, developed during contract performance. The Contractor, in collaboration with VA, must evaluate the output of any AI tool for accuracy prior to using the output in VA efforts. All data, including models, weights, algorithms, and outputs generated using either Government-furnished data or data first developed under this contract shall be the property of the Government with unlimited rights as defined by FAR 52.227-14. The Contractor shall also deliver any custom-developed code developed with AI methodologies in accordance with the SHARE IT Act, if applicable. VA shall also retain unlimited rights to any improvements to that data, including the continued design, development, testing, and operation of AI systems and/or systems utilizing AI.

The Contractor shall ensure that all AI Systems, including Large Language Models (LLM), whether standalone LLMs or integrated into broader software platforms, procured under this effort and/or used in performance of this contract complies with the Unbiased AI Principles as defined in Executive Order 14319 and OMB Memorandum M-26-04, e.g. Truth Seeking and Ideologically Neutral, as applicable to the intended use of the system.

The Contractor shall ensure that AI System/LLM generated outputs are truthful in responding to user prompts seeking factual information or analysis, prioritize historical accuracy, scientific inquiry, and objectivity, as well as acknowledge uncertainty where reliable information is incomplete or contradictory and do not fabricate, hallucinate, or present unverifiable information as fact.

The Contractor shall ensure that LLMs and AI outputs are neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as Diversity, Equity, and Inclusion (DEI). The Contractor shall ensure that the LLMs, including the AI System, are not intentionally encoded with partisan or ideological judgments within an AI System's/LLM's outputs unless those judgments are prompted by or otherwise readily accessible to the end user.

Compliance with the AI requirements of this contract, including adherence to the Unbiased AI Principles, Truth-Seeking and Ideological Neutrality requirements, disclosure obligations, monitoring and reporting requirements, and corrective action responsibilities, is a material condition of eligibility for payment and continued performance. In accordance with OMB Memorandum M-26-04, failure to comply with these requirements, or refusal to take timely and appropriate corrective action to remedy identified noncompliance, may constitute a material breach of contract and may result in remedies consistent with the terms of the contract and applicable law including but not limited to withholding of payment, termination for cause/default, or other appropriate contractual remedies, as determined by the Contracting Officer.

All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation as identified in the Artificial Intelligence in VA Contracts clause, to include its associated list of AI being used in contract performance.

Deliverable:

A. Statement of Attestation

3.7.1 AI SYSTEM/LLM DEVELOPMENT AND OPERATION DOCUMENTATION REQUIREMENTS

To enable Government continued assessment of compliance with Trustworthy AI requirements and both Unbiased AI Principles, Truth-seeking and Ideological Neutrality, in accordance with OMB M-26-04, the Contractor shall provide AI System/LLM Development and Operation Documentation Package to include, at a minimum:

1. **Acceptable Use Policy**
The Contractor shall provide an Acceptable Use Policy document governing its AI operation that characterizes and differentiates appropriate and inappropriate use of their product offering.

2. **Model Cards, System Cards and/or Data Cards**
The Contractor shall provide documentation describing essential information about the model, system, and or data as it relates to the AI/LLM product offering. The documentation shall address summaries of training process, identified risks and mitigations, and model evaluation scores on LLM benchmarks at a minimum, where appropriate.

3. **End User Resources**
The Contractor shall provide documentation to include product tutorials, developer guides, and/or other tools to assist VA in ensuring proper use of the AI/LLM to maximize utility.

4. **Mechanism for End User Feedback**
The Contractor shall provide documentation describing the mechanism employed to provide feedback to the Offeror on outputs identified that violate the Unbiased AI Principles. This may be satisfied by a general inbox, specific Point of Contact, or similar feedback mechanism.

5. **Pre-Training and Post-Training Activities of the AI System/LLM**
The Contractor shall provide documentation of Pre-Training and Post Training Activity that provides details on:
    a. Actions taken that impact the factuality and grounding of AI System/LLM outputs
    b. System-level prompts that provide natural language instructions to the model specifying guidelines on responding to user-generated queries, to include how a model responds when reliable information is incomplete, contradictory, or subject to individual interpretation
    c. The type of outputs restricted via content moderation and safety filters
    d. The use of red teaming as a means of continuously assessing the model to protect against incidents of bias in generated output.
    e. Training or development, if any, that occurred outside the United States, to include the type of activity and the country in which it occurred.
    f. Any modifications or configurations undertaken to comply with any regulation from a government other than the U.S. Federal Government.

6. **Model Evaluation Results and Methodologies**
The Contractor shall provide documentation describing the Evaluation Results of bias evaluations conducted by the Vendor to include the

methodology for performing such tests (e.g., testing prompt pairs for politically oriented topics).

The documentation shall also include Benchmark scoring results measuring the model's bias, helpfulness, honesty, or accuracy when provided with ambiguous versus straightforward questions. (Including any benchmarks comparing performance across multiple languages, where applicable).

7. **Description of Enterprise-Level Controls**
   The Contractor shall provide documentation describing the Enterprise Governance tools and controls, such as:
   a. Customizable system instructions that are additive to a base model's system prompts or content generation filters.
   b. Product features that require a model to cite sources of its outputs or otherwise provide visibility into the provenance of the model's outputs.
   c. AI System/LLM model evaluation tools that enable comparisons either between a model's outputs, or across various models.

8. **Third Party Modification Disclosure**
   The Contractor shall disclose of any additional controls to modify an AI Model's/LLM's output applied by the Contractor if the Contractor is not a direct developer of the LLM (e.g., classifiers, system prompts, fine-tuning, content moderation and filters, etc.)

Deliverable:

A. AI System/LLM Development and Operation Documentation Package

3.7.2 MONITORING, REPORTING, AND CORRECTIVE ACTION

The Contractor shall develop and implement a Compliance Monitoring and Reporting Plan supporting ongoing monitoring processes to evaluate AI outputs for compliance with Trustworthy AI and Unbiased AI principles. This plan shall include the mechanism for authorized users to provide end user feedback to report suspected violations of Truth-Seeking or Ideological Neutrality requirements.

The Contractor shall notify the COR within 10 business days of identifying any material deviation from these principles and shall submit a written Corrective Action Plan describing mitigation steps, responsible parties, and timelines. Any material deviation, corrective action taken, and results shall be detailed in the Monthly Progress Reports.

Deliverable:

A. Compliance Monitoring and Reporting Plan
B. Corrective Action Plan

3.7.3 AI MODEL UPDATES AND CHANGE DISCLOSURES

The Contractor, in an AI Model/LLM Change Disclosure, shall notify the Government throughout the PoP in advance of any material changes to AI models, including new AI enhancements, features and/or components, controls, retraining, classifiers, system prompts, fine-tuning, content moderation, filters, version replacement, or architectural changes, that could reasonably affect compliance with Trustworthy AI or Unbiased AI principles. Updated documentation shall be provided to VA for VA approval prior to implementation of such changes.

Deliverable:

A. AI Model/LLM Change Disclosure

4.0 POINTS OF CONTACT

VA Program Manager:
Will be Provided at Award

Contracting Officer's Representative:
Will be Provided at Award

Contracting Officer:
Name:Mina Awad
Email: Mina.Awad@va.gov

Contract Specialist:
Name:Allison Fulton
Email: Allison.Fulton@va.gov

5.0 INFORMATION SECURITY CONSIDERATIONS

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans and Authority to Operate for all systems/LAN's accessed while performing the tasks detailed in this Product Description.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE

NOTE: In the event of a conflict, VA Acquisition Regulation (VAAR) Security Clauses take precedence over the language in this Addendum B.

APPLICABLE SECTIONS TAILORED FROM: *VA NOTICE 24-12, APRIL 22, 2024, UPDATE TO VA HANDBOOK 6500.6, CONTRACT SECURITY, APPENDIX C VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE*

B1. GENERAL

This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, Subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

B.2 VA INFORMATION CUSTODIAL LANGUAGE

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

b. Information made available to the Contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The Contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

c. VA information will not be co-mingled with any other data on the Contractor’s information systems or media storage systems. The Contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The Contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to Contractor and Subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government

Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The Contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The Contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.

h. The Contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The Contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

i. The Contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The Contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.

k. Notwithstanding the provision above, the Contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality-assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the Contractor is in receipt of a court order or other requests for the above-mentioned information, the

Contractor shall immediately refer such court order or other requests to the VA CO for response.

l. Information made available to the Contractor by VA for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a Contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, Guidelines for Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the Contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The Contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the Contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the Contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of Contractor/Subcontractor and agent of Contractor/Subcontractor.

b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information

systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

c. All Contractors and Subcontractors working with VA information are subject to the same security investigative and clearance requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, Personnel Vetting Program. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

d. All Contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All Contractors and Subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the Contractor must state where all non-U.S. services are provided. The Contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

e. The Contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:

    (1) Contractor/Subcontractor personnel no longer has a need for access to VA information or VA information systems.

    (2) Contractor/Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

    (3) Contractor believes their own personnel or Subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes Contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

    (4) Any previously undisclosed changes to Contractor/Subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

(5) Contractor/Subcontractor personnel have their authorization to work in the United States revoked.

(6) Agreement by which Contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for Contractor personnel.

f. In such cases of contract fulfillment, termination, or other causes; the Contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by Contractor/Subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.

g. Contractors/Subcontractors who no longer require VA accesses will return VA-issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, Contractors shall notify the appropriate VA COR/CO.

B4. TRAINING

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:

(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The Contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.

B5. SECURITY INCIDENT INVESTIGATION

a. The Contractor, Subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the Contractor, Subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

    (1) The date and time (or approximation of) the Security Incident occurred.

    (2) The names of individuals involved (when applicable).

    (3) The physical and logical (if applicable) location of the incident.

    (4) Why the Security Incident took place (i.e., catalyst for the failure).

    (5) The amount of data belonging to VA believed to have been compromised.

    (6) The remediation measures the Contractor is taking to ensure no future incidents of a similar nature.

c. After the Contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The Contractor, Subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT Contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any

possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

f. The Contractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the Contractor is deemed to have discovered a data breach when the Contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract; the Contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).

a. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.

b. VA IT Contractors, Subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, Risk Management Framework for Cloud Computing Services and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly

match VA security requirements, the Contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

c. The Contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-26-05 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change. The term “software” includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The Contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

d. The Contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the Contractor did not develop, all software configurations and all customizations.

e. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.

f. The Contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the Contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the Contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository,

g. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default “program files” directory with silently install and uninstall. The Contractor shall perform testing of all updates and patching prior to implementation on VA systems.

h. Applications designed for normal end users will run in the standard user context without elevated system administration privileges.

i. The Contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.

j. The Contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

k. The Contractor shall comply with the Privacy Act of1974 (the Act), FAR 52.224-2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

l. The Contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as “Information Systems”) throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the Contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The Contractor shall ensure security fixes do not negatively impact the Information Systems.

m. When the Contractor is responsible for operations or maintenance of the systems, the Contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the Contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

a. The Contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated,

maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, change management procedures and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (Contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the Contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The Contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.

c. The Contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The Contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned Contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with Contractor activities are also subject to such assessments. The Contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The Contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The Contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The Contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using government personnel or a third-party if deemed necessary. The Contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or Contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the Contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The Contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved Contractor OE will be subject to technical inspection at any time.

i. The Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

j. For cases wherein the Contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the Contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The Contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the Contractor shall provide the

VA CO/CO written assurance they have permanently remediated these backdoors.

k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

B8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING

a. Should VA request it, the Contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the Contractor's IT or systems and controls, to ascertain whether the Contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the Contractor.

b. Any audits or tests of the Contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact Contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the Contractor uses to destroy, maintain, receive, retain, or use VA information.

c. As part of these audits, tests and assessments, the Contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.

d. The Contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the Contractor has generated as part of its own security assessment. The Contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.

e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The Contractor shall comply with recommendations which result

from these regulatory assessments on the part of VA regulators and associated government agency partners.

B9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING

a. The Contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the Contractor to procure equipment, the Contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The Contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the Contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.

c. All Contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The Contractor shall make spare parts available. All Contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The Contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a Contractor provides software or patches to VA, the Contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The Contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report “The Minimum Elements for a Software Bill of Materials (SBOM).”

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the Contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The Contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

B10. VIRUSES, FIRMWARE, AND MALWARE

a. The Contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The Contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The Contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The Contractor shall provide or arrange for the provision of technical justification as to why any “false positive” hit has taken place to ensure their code’s supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The Contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter “virus or other malware”) onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the Contractor shall:

    (1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and
    (2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

a. The Contractor shall document how the cryptographic system supporting the Contractor’s products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.

b. The Contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.

c. The Contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

d. The Contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.

e. The Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

B12. PATCHING GOVERNANCE

a. The Contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the following:

    (1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and.

    (2) The approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

b. The Contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The Contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by Contractor within these time periods, the Contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The Contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by

Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

B13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING)

a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

b. All Contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the Contractor shall work though the COR/CO for governance or resolution.

c. The Contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the Contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.

d. The Contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Postmarket Management of Cybersecurity in Medical Devices.

e. The Contractor shall design devices capable of accepting all applicable security patches with or without the support of the Contractor personnel. If patching can only be completed by the Contractor, the Contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the Contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The Contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

f. The Contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the Contractor cannot install an anti-virus / anti-malware application.

g. The Contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.

h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the Contractor with media removed. When the contract requires return of equipment, the options available to the Contractor are the following:

(1) The Contractor shall accept the system without the drive, firmware and solid state.

(2) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:

(a) The equipment Contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

B14. DATA CENTER PROVISIONS

a. The Contractor shall ensure the VA network is accessed by in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

b. The Contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

c. The Contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

d. The Contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

e. The Contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

f. The Contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

SECTION C - CONTRACT CLAUSES

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

(End of Clause)

FAR/VAAR Number	Title	Date
52.203-6	Restrictions on Subcontractor Sales to the Government.	JUN 2020
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-13	SYSTEM FOR AWARD MANAGEMENT—MAINTENANCE (DEVIATION)	NOV 2025
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS	DEC 2014
52.209-9	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	NOV 2025
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2025 (DEVIATION)
52.212-4	TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025
52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN	NOV 2025 (DEVIATION)
52.219-16	LIQUIDATED DAMAGES-SUBCONTRACTING PLAN	NOV 2025
52.219-28	POST AWARD SMALL BUSINESS PROGRAM REREPRESENTATION	NOV 2025
52.222-3	CONVICT LABOR	NOV 2025
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	NOV 2025
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES	NOV 2025
52.222-37	EMPLOYMENT REPORTS ON VETERANS	NOV 2025
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NLRA	NOV 2025
52.222-50	COMBATING TRAFFICKING IN PERSONS	NOV 2025
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	NOV 2025
52.224-3	PRIVACY TRAINING	JAN 2017

52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.227-1	AUTHORIZATION AND CONSENT	JUN 2020
52.227-2	PATENT AND COPYRIGHT INFRINGEMENT	JUN 2020
52.228-5	INSURANCE—WORK ON A GOVERNMENT INSTALLATION	JAN 1997
52.232-33	PAYMENT BY EFT - SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	MAR 2023
52.233-1	DISPUTES	MAY 2014
52.233-3	PROTEST AFTER AWARD	NOV 2025 (DEVIATION)
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	NOV 2025 (DEVIATION)
52.240-91	SECURITY PROHIBITIONS AND EXCLUSIONS	(NOV 2025) (DEVIATION)
52.240-93	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS	(NOV 2025) (DEVIATION)
52.242-5	PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	JAN 2017
852.201-70	CONTRACTING OFFICER'S REPRESENTATIVE	DEC 2022
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.204-70	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	MAR 2026 (DEVIATION)
852.219-70	VA SMALL BUSINESS SUBCONTRACTING PLAN MINIMUM REQUIREMENTS	JAN 2023 (DEVIATION)
852.222-71	COMPLIANCE WITH EXECUTIVE ORDER 13899	APR 2025 (DEVIATION)
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.239-70	SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES	FEB 2023
852.239-71	INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION	FEB 2023
852.239-72	INFORMATION SYSTEM DESIGN AND DEVELOPMENT	FEB 2023
852.239-73	INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE	FEB 2023
852.239-74	SECURITY CONTROLS COMPLIANCE TESTING	FEB 2023

C.2 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JUN 2020)

(a) Definitions. As used in this clause—

Agency means “executive agency” as defined in Federal Acquisition Regulation (FAR) 2.101.

Covered Federal action means any of the following actions:
(1) Awarding any Federal contract.
(2) Making any Federal grant.
(3) Making any Federal loan.
(4) Entering into any cooperative agreement.
(5) Extending, continuing, renewing, amending, or modifying any Federal contract, grant, loan, or cooperative agreement.

Indian tribe and “tribal organization” have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b) and include Alaskan Natives.

Influencing or attempting to influence means making, with the intent to influence, any communication to or appearance before—
- an officer or employee of any agency,
- a Member of Congress,
- an officer or employee of Congress, or
- an employee of a Member of Congress

in connection with any covered Federal action.

Local government means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

Officer or employee of an agency includes:
(1) Individuals appointed under Title 5, U.S.C., including temporary appointments.
(2) Members of the uniformed services, as defined in 37 U.S.C. 101(3).
(3) Special Government employees (18 U.S.C. 202).
(4) Members of a Federal advisory committee (5 U.S.C., app. 2).

Person means an individual, corporation, company, association, authority, firm, partnership, society, State, or local government, for-profit or not-for-profit.

This term excludes an Indian tribe, tribal organization, or other Indian organization with respect to expenditures specifically permitted by other Federal law.

Reasonable compensation means, with respect to a regularly employed officer or employee, compensation consistent with normal compensation for such officer or employee for work not furnished to, funded by, or in cooperation with the Federal Government.

Reasonable payment means, with respect to professional and other technical services, a payment consistent with amounts normally paid in the private sector.

Recipient includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans, but only with respect to expenditures described in paragraph (b) of this clause permitted by other Federal law.

Regularly employed means, with respect to an officer or employee, one employed for at least 130 working days in the year preceding the proposal submission. Less than 130 days is not considered regularly employed until the 130th day.

State means a U.S. State, the District of Columbia, an outlying area, or an agency or instrumentality thereof, including multi-State, regional, or interstate entities with governmental duties and powers.

(b) Prohibition. 31 U.S.C. 1352 prohibits use of appropriated funds to pay any person to influence Federal officers, employees, or Members of Congress in connection with any covered Federal action. The Contractor shall not use appropriated funds for these purposes in connection with this contract.

(1) “Appropriated funds” excludes profit or fee from a covered Federal action.
(2) If the Contractor has non-Federal funds sufficient to cover influencing activities, the Government will assume those funds were used.

(c) Exceptions. The prohibition does not apply to:
(1) Agency and legislative liaison by Contractor employees, including:
(i) Reasonable compensation for liaison not directly related to this contract—including responding to agency or Congressional requests, discussing general product/service capabilities, providing unsolicited information to start a covered action, technical discussions on unsolicited proposals, or small business capability presentations.
(2) Professional and technical services—payments for such services rendered directly in the preparation, submission, or negotiation of proposals or to meet legal requirements, including those to consultants or trade associations.
(3) Only the communications and services expressly permitted above are allowed.

(d) Disclosure.
(1) If OMB Standard Form LLL was not submitted with the offer, but lobbying activity occurred, the Contractor must submit it to disclose the registrants.
(2) If previously submitted, any change affecting Block 10 of Form LLL requires submission of an updated form within 30 days of the end of the quarter in which the change occurs.

(e) Penalties.
(1) Violations of paragraph (b) or failure to file or amend disclosure as required in (d) may result in civil penalties under 31 U.S.C. 1352, in addition to other remedies.
(2) Contractors may rely on subcontractor representations without liability.

(f) Cost allowability. This clause does not make unallowable costs allowable, nor make allowable costs unallowable under other provisions.

(g) Subcontracts.

(1) The Contractor must obtain declarations—including certification and disclosure per FAR 52.203-11—from subcontractors exceeding the FAR 3.808 threshold.
(2) Subcontractor disclosure forms are forwarded tier to tier until the prime Contractor receives them.
(3) The substance of this clause must be included in all applicable subcontracts.

(End of clause)

C.3 52.209-6 Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded.

As prescribed in 9.409 , insert the following clause:

PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED (Nov 2025)

(a) *Definition*. As used in this clause—
Commercially available off-the-shelf (COTS) item
(1) Means any item of supply (including construction material) that is–
(i) A commercial product (as defined in paragraph (1) of the definition of “commercial product” in Federal
Acquisition Regulation (FAR) 2.101);
(ii) Sold in substantial quantities in the commercial marketplace; and
(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form
in which it is sold in the commercial marketplace; and
(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum
products.
(b) The Government suspends or debars Contractors to protect the Government's interests. Other than a subcontract for
a commercially available off-the-shelf item, the Contractor shall not enter into any subcontract, in excess of the threshold
specified in FAR 9.405-2(b) on the date of subcontract award, with a Contractor that is debarred, suspended, or proposed for
debarment by any executive agency unless a compelling reason exists to do so.
(c) The Contractor shall require each proposed subcontractor whose subcontract will exceed the threshold specified in
FAR 9.405-2(b) on the date of subcontract award, other than a subcontractor providing a commercially available off-the-shelf
item, to disclose to the Contractor, in writing, whether as of the time of award of the subcontract, the subcontractor, or its
principals, is or is not debarred, suspended, proposed for debarment, or voluntarily excluded by the Federal Government.
(d) A corporate officer or a designee of the Contractor shall notify the Contracting Officer, in writing, before entering

into a subcontract with a party (other than a subcontractor providing a commercially available off-the-shelf item) that is
debarred, suspended, proposed for debarment, or voluntarily excluded (see FAR 9.404 for information on the System for
Award Management (SAM) Exclusions). The notice must include the following:
(1) The name of the subcontractor.
(2) The Contractor's knowledge of the reasons for the subcontractor being listed with an exclusion in SAM.
(3) The compelling reason(s) for doing business with the subcontractor notwithstanding its being listed with an
exclusion in SAM.
(4) The systems and procedures the Contractor has established to ensure that it is fully protecting the Government's
interests when dealing with such subcontractor in view of the specific basis for the party's debarment, suspension, proposed
debarment, or voluntary exclusion.
(e) *Subcontracts*. Unless this is a contract for the acquisition of commercial products or commercial services, the
Contractor shall include the requirements of this clause, including this paragraph (e) (appropriately modified for the
identification of the parties), in each subcontract that—
(1) Exceeds the threshold specified in FAR 9.405-2(b) on the date of subcontract award; and
(2) Is not a subcontract for commercially available off-the-shelf items.

(End of clause)

C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor at any time prior to expiration of the period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend before the Order expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years.

(End of Clause)

C.5 52.219-8 UTILIZATION OF SMALL BUSINESS CONCERNS

As prescribed in 19.708(a), insert the following clause:

a) *Definitions*. As used in this contract—

HUBZone small business concern means a small business concern that meets the requirements described in 13 CFR 126.200, certified by the Small Business Administration (SBA) and designated by SBA as a HUBZone small business concern in the Dynamic Small Business Search (DSBS) and SAM.

Service-disabled veteran-owned small business (SDVOSB) concern means a small business concern—

(1)

(i) Not less than 51 percent of which is owned and controlled by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran; or

(2) A small business concern eligible under the SDVOSB Program in accordance with 13 CFR part 128 (see subpart 19.14).

(3) Service-disabled veteran, as used in this definition, means a veteran, as defined in 38 U.S.C.101(2), with a disability that is service-connected, as defined in 38 U.S.C.101(16), and who is registered in the Beneficiary Identification and Records Locator Subsystem, or successor system that is maintained by the Department of Veterans Affairs' Veterans Benefits Administration, as a service-disabled veteran.

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that—

(1) Effective January 1, 2024, is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300; or

(2) Has represented that it is an SDVOSB concern in SAM and submitted a complete application for certification to SBA on or before December 31, 2023.

Service-disabled veteran-owned small business (SDVOSB) Program means a program that authorizes contracting officers to limit competition, including award on a sole-source basis, to SDVOSB concerns eligible under the SDVOSB Program.

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation and qualified as a small business under the criteria and size standards in 13 CFR part 121, including the size standard that corresponds to the NAICS code assigned to the contract or subcontract.

Small disadvantaged business concern, consistent with 13 CFR 124.1001, means a small business concern under the size standard applicable to the acquisition, that-

(1) Is at least 51 percent of which is owned and controlled (as defined at 13 CFR 124.105) by-

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding the threshold at 13 CFR 124.104(c)(2) after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Veteran-owned small business concern means a small business concern-

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C.101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned small business concern means a small business concern-

(1) That is at least 51 percent owned by one or more women, or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(b) It is the policy of the United States that small business concerns, veteran-owned small business concerns, service-disabled veteran-owned small business concerns, HUBZone small business concerns, small disadvantaged business concerns, and women-owned small business concerns shall have the maximum practicable opportunity to participate in performing contracts let by any Federal agency, including contracts and subcontracts for subsystems, assemblies, components, and related services for major systems. It is further the policy of the United States that its prime contractors establish procedures to ensure the timely payment of amounts due pursuant to the terms of their subcontracts with small business concerns, veteran-owned small business concerns, service-disabled veteran-owned small business concerns, HUBZone small business concerns, small disadvantaged business concerns, and women-owned small business concerns.

(c)

(1) A joint venture qualifies as a small business concern if—

(i) Each party to the joint venture qualifies as small under the size standard for the solicitation; or

(ii) The protégé is small under the size standard for the solicitation in a joint venture comprised of a mentor and protégé with an approved mentor-protégé agreement under a SBA mentor-protégé program. (See 13 CFR 125.9(d).)"; and

(2) A joint venture qualifies as a HUBZone small business concern if it complies with the requirements in 13 CFR 126.616(a) through (c).

(d) The Contractor hereby agrees to carry out this policy in the awarding of subcontracts to the fullest extent consistent with efficient contract performance. The Contractor further agrees to cooperate in any studies or surveys as may be conducted by the United States Small Business Administration or the awarding agency of the United States as may be necessary to determine the extent of the Contractor's compliance with this clause.

(e)

(1) Unless the Contractor has reason to question the representation, it may accept a subcontractor's written representations of its size and socioeconomic status as a small business, small disadvantaged business, veteran-owned small business, service-disabled veteran-owned small business, or a women-owned small business if the subcontractor represents that the size and socioeconomic status representations with its offer are current, accurate, and complete as of the date of the offer for the subcontract.

(2) Unless the Contractor has reason to question the representation, it may accept a subcontractor's representations of its size and socioeconomic status as a small business, small disadvantaged business, veteran-owned small business, service-disabled veteran-owned small business, or a women-owned small business in the System for Award Management (SAM) if—

(i) The subcontractor is registered in SAM; and

(ii) The subcontractor represents that the size and socioeconomic status representations made in SAM are current, accurate and complete as of the date of the offer for the subcontract.

(3) The Contractor may not require the use of SAM for the purposes of representing size or socioeconomic status in connection with a subcontract.

(4) In accordance with 13 CFR 121.411, 126.900, 127.700, and 128.600, a contractor acting in good faith is not liable for misrepresentations made by its subcontractors regarding the subcontractor's size or socioeconomic status.

(5) The Contractor shall confirm that a subcontractor representing itself as a HUBZone small business concern is certified by SBA as a HUBZone small business concern by accessing SAM or by accessing DSBS at https://web.sba.gov/pro-net/search/dsp_dsbs.cfm. If the subcontractor is a joint venture, the Contractor shall confirm that at least one party to the joint venture is certified by SBA as a HUBZone small business concern. The Contractor may confirm the representation by accessing SAM.

(End of Clause)

C.6 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026)

(a)Definitions. As used in this clause—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph

(c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of Clause)

C.7 852.211-76 LIQUIDATED DAMAGES – REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023) ALTERNATE I (FEB 2023)

As prescribed in 811.503-70, insert the following clause:

Liquidated Damages—Reimbursement for Data Breach Costs (FEB 2023)

(a) *Definition.* As used in this clause, “contract” means any contract, agreement, order or other instrument and encompasses the definition set forth in FAR 2.101.

(b) *Non-disclosure requirements.* As a condition of performance under a contract, order, agreement, or other instrument that requires access to sensitive personal information as defined in VAAR 802.101, the following is expressly required—

(1) The Contractor, subcontractor, their employees or business associates shall not, directly or through an affiliate or employee of the Contractor, subcontractor, or business associate, disclose sensitive personal information to any other person unless the disclosure is lawful and is expressly permitted under the contract; and

(2) The Contractor, subcontractor, their employees or business associates shall immediately notify the Contracting Officer and the Contracting Officer's Representative (COR) of any security incident that occurs involving sensitive personal information.

(c) *Liquidated damages.* If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of $37.50 per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. In the event the Contractor provides payment of actual damages in an amount determined to be adequate by the Contracting Officer, the Contracting Officer may forgo collection of liquidated damages.

(d) *Purpose of liquidated damages.* Based on the results from VA's determination that there was a data breach caused by Contractor's or any of its agents' failure to protect or otherwise engaging in conduct to cause a data breach of VA sensitive personal information, and as directed by the Contracting Officer, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of the following:

(1) Notification related costs.

(2) Credit monitoring reports.

(3) Data breach analysis and impact.

(4) Fraud alerts.

(5) Identity theft insurance.

(e) *Relationship to termination clause, if applicable.* If the Government terminates this contract, purchase order, or agreement, in whole or in part under clause 52.249-8, Default—Fixed-Price Supply and Service, or any other related FAR or VAAR clause included in the contract, in addition to the required liquidated damages for data breach-related expenses specified in paragraph (c) above, the Contractor is liable for excess costs for those supplies and services for repurchase as may be required under the Termination clause.

(End of clause)

Alternate I (FEB 2023). In commercial products or commercial services acquisitions awarded under the procedures of FAR part 8 or 12, substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable.* If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.212-4(m), Contract Terms and Conditions—Commercial Products and Commercial Services, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

Alternate II (FEB 2023). In simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial products or commercial services awarded under the procedures of FAR part 13 (*see* FAR 13.302-5(d)(1) and the clause at FAR 52.213-4), substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable.* If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.213-4(g), Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services), or any other applicable FAR or VAAR clause, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

(End of Clause)

C.8 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY

As prescribed in 839.203-70(b), insert the following clause:

INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023)

(a) All information and communication technology (ICT) (formerly referred to as electronic and information technology (EIT)) supplies, information, documentation and

services support developed, acquired, maintained or delivered under this contract or order must comply with the ‘‘Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards’’ (see 36 CFR part 1194). Information about Section 508 is available at http://www.section508.va.gov/.
(b) The Section 508 accessibility standards applicable to this contract or order are identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
(c) The Section 508 accessibility standards applicable to this contract are located in Paragraph 2.1 of the PD, as located in Section B.

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the Contractor submit a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
(e) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

NONE

SECTION E - SOLICITATION PROVISIONS

E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

(End of Provision)

FAR/VAAR Number	Title	Date
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS	JAN 2017
52.204-5	WOMEN-OWNED BUSINESS (OTHER THAN SMALL BUSINESS)	OCT 2014
52.204-7	SYSTEM FOR AWARD MANAGEMENT—REGISTRATION (DEVIATION)	NOV 2025
52.209-2	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS--REPRESENTATION	NOV 2025
52.212-1	INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025
52.217-5	EVALUATION OF OPTIONS	NOV 2025
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION	JUN 2020
852.215-72	NOTICE OF INTENT TO RE-SOLICIT	OCT 2019
852.233-70	PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION	OCT 2018
852.233-71	ALTERNATIVE PROTEST PROCEDURE	OCT 2018
852.239-71	INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION	FEB 2023
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023
52.240-90	SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS	NOV 2025

E.2 FAR 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (NOV 2025 (DEVIATION))

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals—

(A) Are □ are not □ presently debarred, suspended, proposed for debarment, or declared ineligible for the award
of contracts by any Federal agency;

(B) Have □ have not □, within a three-year period preceding this offer, been convicted of or had a civil judgment
rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or
performing a public (Federal, State, or local) contract or subcontract; violation of Federal or State antitrust statutes relating
to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records,
making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property (if offeror checks
"have", the offeror shall also see 52.209-7, if included in this solicitation);

(C) Are □ are not □ presently indicted for, or otherwise criminally or civilly charged by a governmental entity
with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision; and

(D) Have □, have not □, within a three-year period preceding this offer, been notified of any delinquent Federal
taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied. Federal taxes are
considered delinquent if both of the following criteria apply:

(1) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability
is not finally determined if a pending administrative or judicial challenge remains. In the case of a judicial challenge to the
liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(2) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay
the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection
action is precluded.

(ii) The Offeror has □ has not □, within a 3-year period preceding this offer, had one or more contracts terminated

for default by any Federal agency.

(2) "Principal," for the purposes of this certification, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the Government will consider the certification in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) This provision does not require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a). The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If the Government later determines that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of provision)

E.3 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (NOV 2025)

(a) *Definitions.* As used in this provision—
"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—
(1) The total value of all current, active contracts and grants, including all priced options; and
(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).
"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.
(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.
(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or
(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.
(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via *https://www.sam.gov* (see 52.204-7).

(End of Provision)

E.4 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (FEB 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that–
(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or
(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.
(b) The Offeror represents that–
(1) It is □ is not □ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and
(2) It is □ is not □ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

E.5 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION)
The Government contemplates award of a Firm-Fixed-Price contract resulting from this solicitation.

(End of Provision)

E.6 52.233-2 SERVICE PROTEST (NOV 2025)

(a) Protests, (as defined in FAR 33.102), that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), must be served on the Contracting Officer identified in the solicitation by obtaining written and dated acknowledgment of receipt from them.

Email: Mina.awad@va.gov

(b) The copy of any protest must be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.7 BASIS FOR AWARD

Award will be made to the lowest priced, responsive, responsible offeror whose quote conforms to the requirements of the solicitation set forth in the Price Schedule and Product Description, Section B.4 and B.5. Eligibility for award is limited to Offerors who have an active registration in the System for Award Management (SAM) at time of submission of the quote. Accordingly, quotes submitted by Offerors that do not meet the SAM certification requirements will not be evaluated.

The Government will evaluate offers for award purposes by adding the total price for all items in the price schedule. The total evaluated price will be that sum.

E.8 QUOTE SUBMISSION INSTRUCTIONS

All quotes shall be subject to evaluation by a team of Government personnel. The Government intends to award without exchanges based upon the initial evaluation of quotes.

Quotes shall be submit via email with your company information to Contract Specialist, Allison.Fulton@va.gov and Contracting Officer, Mina.Awad@va.gov. Please note that file size is limited to less than 5 mb. If your file exceeds the size limit, please send multiple emails.

Your response must be received by the closing date indicated on the SAM.gov website for the quote which is also noted in Blocks 6 and 8 of the SF1449, to be considered timely for award of an Order. Multiple quotes are not permitted and shall not be considered for award. The use of hyperlinks or embedded attachments in quotes is prohibited. Accordingly, any information contained within an embedded attachment and/or hyperlink will neither be accessed nor evaluated.

The quote shall be submitted in accordance with FAR 52.212-1 as supplemented by the below:

Offerors shall complete Section B.4, Price Schedule, with prices for all items in the solicitation and submit with their quote; if none enter $0. All prices shall contain no more than two decimal places. For each priced line item ensure the “Unit price” column multiplied by the “Quantity” column equals the “Total Price” column.

Offerors must meet all the requirements listed in the Price Schedule and Product Description and have each requirement outlined in their quote to include a description of the items being offered in sufficient detail to evaluate conformance with the requirements in the solicitation. No assumptions of compatibility will be made on part of the VA. Failure to list all requirements in their entirety in an Offeror’s quote will result in a noncompliant quote.

Offerors must submit a quote on an “all or none” basis. All Offerors are cautioned that any deviation from the Government’s minimum terms and conditions set forth in this

Solicitation may result in your offer being deemed by the Government to be non-conforming to the requirements and excluded from consideration for award.

Accordingly, Offerors are hereby advised that any Offeror-imposed terms and conditions and/or assumptions which deviate from the Government's material terms and conditions established by the Solicitation, may render the Offeror's quote Unacceptable, and thus ineligible for award. This may include, but is not limited to, quotes predicated on incorporation of commercial software license agreements.

In addition, the Offeror shall provide with its quote a Certification Letter from the Original Equipment Manufacturer (OEM) for any and all proposed products listed in the Section B, Price Schedule certifying that both the Respondent and any pass-through vendors, are authorized to sell and provide the proposed product(s) as of the date of the submission of the quote/proposal. The Letter(s) shall be provided on official letterhead, as required by the OEM(s), to support authorized product sale and pricing for the products proposed. Failure to include the requisite Letter(s) may render the Respondent's quote Unacceptable and thus, ineligible for award.

(End of Provision)