**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: 36C10B26R0020

6. SOLICITATION ISSUE DATE: 06-11-2026

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: Juan C Perez

b. TELEPHONE NO. (No Collect Calls): 512-981-4467

8. OFFER DUE DATE/LOCAL TIME: 07-13-2026 14:00 EDT

9. ISSUED BY — CODE

Department of Veterans Affairs
Technology Acquisition Center
Procurement Services G
23 Christopher Way
Eatontown NJ 07724

10. THIS ACQUISITION IS

- [ ] UNRESTRICTED OR
- [X] SET ASIDE: 100 % FOR:
- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [X] 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 Employee

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 Delivery Schedule

Eatontown NJ 07724

16. ADMINISTERED BY — CODE

Department of Veterans Affairs
Technology Acquisition Center
Procurement Services G
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

Department of Veterans Affairs
Technology Acquisition Center
Financial Services Center
PO Box 149971
Austin TX 78714-8971

PHONE: — 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 |
|---|---|---|---|---|---|
| | Patient Elopement Prevention<br><br>See Continuation Page<br><br>(Use Reverse and/or Attach Additional Sheets as Necessary) | | | | |

25. ACCOUNTING AND APPROPRIATION DATA

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

- [X] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA — [X] 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): Edgar Alonso-Bernal

31c. DATE SIGNED

## B.1 Schedule of Supplies/Services

| Item # | Description/Part Number | Unit | Quantity | Price | Total |
|---|---|---|---|---|---|
| 1. Specific requirements are detailed in Section B.4, Performance Work Statement (PWS) titled "Patient Elopement Prevention Systems", dated April 27, 2026.<br><br>2. ARM Number: TBD<br><br>3. Inspection/Acceptance/FOB: Destination.<br><br>4. Address/Point of Contact: See B.4 Product Description.<br><br>5. Ordering shall be conducted through the process described in B.6, "Ordering Procedures" and payment shall be made in accordance with Section B.3, Paragraph "Accounting and Appropriation Data."<br><br>6. Pricing shall be placed in accordance with Attachment A. | | | | | |
| | | | | **Total Contract Ceiling** | **$5,000,000** |

## Governing Law Clause

Federal law and regulations, including the Revolutionary Federal Acquisition Regulation (FAR) Overhaul (RFO), 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 RFO 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 RFO 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 RFO 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.

**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 RFO 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 RFO 52.212-4(e).
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 RFO 52.212-4(e); 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.

## USE OF ARTIFICIAL INTELLIGENCE

The Contractor (or subcontractor at any tier, including affiliates) shall not use, sell, monetize, or otherwise release or misuse any VA data, models, training/testing data, patterns, documentation, implementation artifacts, runtime artifacts, and/or any other digital artifacts, partially or in whole, derived from AI or machine learning without the express written consent and approval from the VA Contracting Officer.

The Contractor shall indemnify VA and its officers, employees, and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of VA use of any AI products and/or services under the contract.

The Contractor shall maintain commercially reasonable and industry standard conforming security safeguards and controls, including proper access controls for the AI. The Contractor agrees the VA Contracting Officer has the unilateral right to require deactivation of any AI for any reason without notice.

Any development and/or creation of AI, or AI derivatives and/or data, is subject to all applicable intellectual property and data rights clauses under the contract.

Non-compliance with any of the above terms, or an accidental or purposeful loss of sensitive VA medical records information resulting from AI use, may result in liability to VA for any and all rights and remedies provided by law, including but not limited to contract termination, liquidated damages, and referral to VA's Suspension and Debarment Committee. The Contractor shall include the substance of this clause in in all subcontracts, including subcontractors at any tier and affiliates.

## B.2 CONTRACT ADMINISTRATION DATA

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

   a. CONTRACTOR: See Block 17a

   b. GOVERNMENT: Contracting Officer - See Block 31b
   Department of Veterans Affairs
   Technology Acquisition Center-Austin
   23 Christopher Way
   Eatontown, NJ 07724

2. 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

3. INVOICES: Invoices shall be submitted in arrears:

   a. Quarterly []
   b. Semi-Annually []
   c. Other [X – Upon acceptance]

4. 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.

   See website at: http://www.fsc.va.gov/einvoice.asp

## B.3 ACCOUNTING AND APPROPRIATION DATA

Funding will be identified on the individual task orders executed against this contract.

## B.4 PRODUCT DESCRIPTION

# PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

**Veteran Health Administration**

**Patient Elopement Prevention Systems**

**Date: April 27, 2026**

**TAC- VA-26-00049526**

**PWS Version Number: 2**

## 1.0 BACKGROUND:

The mission of the Department of Veterans Affairs (VA) is to deliver benefits and services to United States Veterans. In fulfilling this mission, VA is committed to providing high-quality, effective, and efficient operational support to those responsible for caring for Veterans—both at the point of care and across every stage of their healthcare journey — in a timely, compassionate, and impactful manner.
A critical component of this mission is patient safety, particularly for vulnerable populations such as those in Community Living Centers (CLCs), Emergency Departments (ED), inpatient units, and Behavioral Health settings. These patients may be at risk of elopement, wandering, or unauthorized exit, which can lead to disruption of care and severe harm. Preventing such incidents is a Joint Commission priority and an essential part of VA's commitment to zero harm.

To achieve this, VA Health Care Systems (HCS) currently utilize proprietary patient elopement and wandering (PEW) prevention technologies from two manufacturers: CenTrak® and Securitas Healthcare®. These systems enable continuous electronic supervision, real-time alerts, and workflow integration to reduce adverse events and improve staff response times.

The goal of this requirement is to maintain, expand, and standardize PEW prevention technology across seven healthcare systems. VA aims to deliver a consistent, interoperable, and scalable patient safety solution that meets clinical, operational, and regulatory requirements across these diverse facilities.

## 2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. "Federal Information Security Modernization Act of 2014"
2. Federal Information Processing Standards (FIPS) Publication 140-3, "Security Requirements for Cryptographic Modules", March 22, 2019
3. FIPS Pub 199. "Standards for Security Categorization of Federal Information and Information Systems," February 2004
4. FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
5. FIPS Pub 201-3, "Personal Identity Verification of Federal Employees and Contractors," January 2022
6. 10 U.S.C. § 2224, "Defense Information Assurance Program", as amended
7. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
8. Public Law 109-461 (P.L. 109-461), Veterans Benefits, Health Care, and Information Technology Act of 2006, as amended, Title IX, Information Security Matters
9. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964", as amended
10. VA Directive 0710, "Personnel Vetting Program," September 8, 2025, https://www.va.gov/vapubs/index.cfm
11. VA Handbook 0710, "Personnel Vetting Program," September 8, 2025, https://www.va.gov/vapubs/index.cfm

12. VA Directive 6102, “Internet/Intranet Services,” August 5, 2019
13. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” as amended
14. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
15. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”, as amended
16. NIST SP 800-66 Rev. 2, “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,” February 2024
17. 45 C.F.R Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 C.F.R. Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”); as amended
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021 (see VA NOTICE 24-18, dated September 27, 2024, “Update to VA Directive 6500 Cybersecurity Program”, and VA Notice 25-07, dated 3/18/25, “Amending VA Directive 6500 to incorporate M-24-15”)
21. VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021 (see VA Notice 25-01, dated October 15, 2024, “Update to VA Handbook 6500 Risk Management Framework for VA Information Systems VA Information Security Program”, and VA Notice 25-06, dated 3/18/25, “Amending VA Directive 6500 to incorporate M-24-15”, VA Notice 25-16, dated September 15, 2025, “Amending VA Handbook 6500 to Replace Enterprise Mission Assurance Support Services Tool With Office of Information Technology Governance Risk Compliance Tool, and VA Notice 25-17, dated September 22, 2025, “Rescission Of Office Of Information Security (OIS) Deputy Assistant Secretary (DAS) Memorandum – Requirements of Proper Plan of Action and Milestones (POA&M) Completion)
22. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” June 30, 2023
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010 (see VA Notice 24-12, dated 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”)
24. VA Handbook 6500.8, “Information System Contingency Planning,” March 25, 2025
25. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018 (see VA NOTICE 25-10, dated June 9, 2025, “Use of Personally Owned Mobile Devices Policy Amendment of Department of Veterans Affairs Handbook 6500.10”, and VA Notice 25-15, dated August 22, 2025, “Update to VA Handbook 6500.10 Mobile Device Security Policy”)
26. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
27. OIT Process Asset Library (PAL), OIT Process Asset Library.
28. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
29. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
30. VA Directive 6510, “VA Identity, Credential and Access Management,” September 3, 2024
31. VA Handbook 6510, “VA Identity, Credential and Access Management,” September 27, 2024
32. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
33. VA Directive 6300, “Records and Information Management,” September 21, 2018
34. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010

35. NIST SP 800-37 Rev 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018
36. NIST SP 800-53 Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” September 23, 2020 (includes updates as of 12/10/2020)
37. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
38. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
39. OMB Memorandum 05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005
40. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
41. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
42. Federal Identity, Credential, and Access Management (FICAM) Architecture, June 30, 2023 (FICAM Architecture (idmanagement.gov))
43. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
44. NIST SP 800-63 Rev 4, 800-63A-4, 800-63B-4, 800-63C-4, “Digital Identity Guidelines,” August 1, 2025
45. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
46. VA Memorandum, VAIQ #7100147, “Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12),” April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896
49. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, https://www.cisa.gov/publication/tic-30-core-guidance-documents
50. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
51. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (P.L. 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (P.L. 109–58), August 8, 2005
54. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
55. Executive Order 14148, “Initial Rescissions of Harmful Executive Orders and Actions,” dated January 20, 2025
56. VA Directive 0057, “VA Environmental Management Program,” October 25, 2022
57. OIS VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
58. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
59. “Veteran Focused Integration Process (VIP) Guide 4.0,” March 2021, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
60. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

61. "Product Line Management Transformation Playbook" version 3.1, August 2023, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946
62. NIST SP 500-267B Revision 1, "USGv6 Profile," November 2020
63. OMB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," November 19, 2020
64. Social Security Number (SSN) Fraud Prevention Act of 2017
65. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018
66. C.F.R Title 15 Part 7, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain", as amended
67. Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/
68. OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
69. NIST SP 800-52 Revision 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
70. OMB M-26-05, "Adopting a Risk-based Approach to Software and Hardware Security," January 23, 2026
71. OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," August 27, 2021
72. NIST SP 800-88 Revision 1 "Guidelines for Media Sanitization," December 2014
73. CISA Binding Operational Directive (BOD) 19-02: "Vulnerability Remediation Requirements of Internet-Accessible Systems," April 29, 2019, BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems | CISA
74. CISA BOD 22-01: "Reducing the Significant Risk of Known Exploited Vulnerabilities," November 3, 2021, BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA
75. CISA BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks." Cybersecurity & Infrastructure Security Agency (CISA), BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks | CISA
76. VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, June 03, 2019
77. VA Memorandum, "VA Security Controls," January 17, 2025, https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010
78. E.O. 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," December 3, 2020
79. E.O. 14319, "Preventing Woke AI in the Federal Government," July 23, 2025
80. OMB Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," April 3, 2025
81. OMB Memorandum M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government," April 3, 2025
82. OMB Memorandum M-26-04, "Increasing Public Trust in Artificial Intelligence (AI) Through Unbiased AI Principles," December 11, 2025

## 3.0 SCOPE OF WORK:

The Contractor shall provide the professional services, hardware, and software required for the maintenance, expansion, and integration of patient elopement and wandering (PEW) prevention systems across our HCS(s). The scope includes the following:

- **Technology and Project Management**: The Contractor shall develop and maintain a master project plan, coordinate stakeholder engagement, provide reporting, and track key performance indicators (KPIs) such as location accuracy, alarm response times, and system uptime.

- **Requirements and System Design**: The Contractor shall conduct workflow discovery and produce architecture for the PEW prevention systems, including coverage maps, geofencing zones, and per-patient security profiles.

- **Delivery and Staging**: The Contractor shall manage hardware/software staging, perform pre-configuration, and validate interoperability among components.

- **Installation and Deployment**: The Contractor shall ensure site readiness and perform hardware installation (e.g., readers, gateways, LF chokepoints, Wi-Fi tags, BLE beacons), patient tagging, and zone configuration.

- **Integration with Enterprise Systems**: The Contractor shall configure integrations with enterprise platforms such as nurse call systems, fire alarm systems, and access control systems to enable event-driven alerts and secure workflows.

- **BLE Enablement**: The Contractor shall implement beacon placement strategies, calibrate for accuracy, integrate gateways, and enable mobile app functionality (if applicable) for real-time notifications.

- **Data Governance and Cybersecurity**: The Contractor shall ensure HIPAA compliance, encryption, adherence to VA security standards, and support VA Enterprise Risk Analysis (ERA) processes.

- **Testing and Validation**: The Contractor shall perform factory and site acceptance tests, verify accuracy and alarm detection, conduct performance and failover testing, and validate data integrity.

- **Training and Change Management**: The Contractor shall deliver role-based training, provide Standard Operating Procedures (SOPs) and job aids, ensure Section 508 compliance, and implement adoption strategies with OEM clinical educator support.

- **Operations and Sustainment**: The Contractor shall implement a tiered support model with SLAs, provide preventive and corrective maintenance, monitor system health, and conduct optimization reviews.

- **Documentation and Deliverables**: The Contractor shall provide design diagrams, configuration baselines, test reports, operational manuals, and disaster recovery plans.

- **System Health and Analytics**: The Contractor shall deploy dashboards for device uptime, tag battery status, location accuracy, alarm metrics, utilization trends, and predictive analytics for workflow optimization.

### 3.1 PERFORMANCE OBJECTIVES:

- **Objective 1**: The Contractor shall deliver a unified PEW enterprise architecture that addresses VISN-wide operational, clinical, and technical requirements. This objective includes conducting comprehensive workflow discovery, facility assessments, and technical analyses to document current-state conditions across multiple sites. In addition, the resulting architecture must incorporate standardized clinical workflows, common geofencing strategies, uniform alarm routing rules, and harmonized data models that promote consistency and interoperability across VISN 21. The enterprise architecture shall be scalable, support modern RTLS/BLE capabilities, comply with VA infrastructure standards, and provide a foundation for long-term modernization and future enhancements.

- **Objective 2**: The Contractor shall provide a comprehensive transition pathway from all existing PEW systems currently deployed across VISN 21 (Table 1) to the proposed solution. This shall include a detailed migration strategy, risk mitigation approach, interoperability plan, and schedule that ensures continuity of operations and prevents disruption to patient safety workflows. The Contractor must identify required technical adaptations, data migration steps, integration changes, and interim support measures needed to maintain full functionality of legacy systems throughout the transition. The pathway shall enable a controlled, phased, and fully supported migration that preserves operational readiness while achieving alignment with the proposed enterprise PEW prevention platform.

- **Objective 3**: Implement, configure, and validate the standardized enterprise solution once designed, ensuring installations are aligned with VISN requirements and tailored to site-specific operational environments. This includes deployment and calibration of hardware components such as readers, gateways, exciters, beacons, and controllers; configuration of software platforms, user interfaces, and alarm logic; execution of facility-specific tuning for accuracy and zone detection; and system optimization to ensure performance expectations are met. The objective also includes comprehensive acceptance testing—such as performance testing, interference checks, accuracy validation, and user acceptance testing—to confirm that the system meets clinical, operational, and technical needs across all VISN 21 facilities.

- **Objective 4**: Ensure that all system components comply with applicable VA cybersecurity requirements. This objective includes implementing FIPS-validated

encryption for data at rest and in transit, ensuring PIV-authenticated access for system users, validating authoritative data source integration requirements, and aligning all applications and hardware with VA Technical Reference Model standards. It also encompasses compliance with VA's identity and access management frameworks, vulnerability remediation timelines, OS and application patching requirements, and accessibility standards for all user-facing interfaces and documentation.

- **Objective 5**: Provide comprehensive training, documentation, and transition support to ensure VISN 21 staff are prepared to operate and maintain the standardized system long term. This includes developing and delivering role-based training for clinical, security, biomedical engineering, OIT, and administrative staff; preparing user guides, technical manuals, SOPs, and job aids; documenting all system configurations, workflows, and maintenance procedures; and executing a structured transition plan with a clearly defined Responsible, Accountable, Consulted, and Informed (RACI) model. The goal is to establish VISN-wide competency and self-sufficiency, ensuring that each facility can support routine operations, respond effectively to alarms, manage patient tagging workflows, and sustain the enterprise system after the period of performance.

## 3.2 TEAMING AND RESELLER REQUIREMENTS:

The Contractor shall maintain formal teaming agreements or authorized reseller/distributor status with the Original Equipment Manufacturers (OEM) for all proposed hardware, software, and professional services throughout the entire Ordering Period. Offerors must demonstrate the ability to obtain required OEM agreements prior to performance and must provide proof of OEM authorization during the contract kickoff meeting. The Contractor shall ensure that all OEM partnerships grant full rights to procure, configure, install, integrate, and support the proposed solutions, including access to OEM technical resources, firmware updates, and warranty services. Failure to maintain OEM authorization or teaming agreements during the POP may result in termination for cause.

## 4.0 PERFORMANCE DETAILS:

This is an Indefinite Delivery/Indefinite Quantity (IDIQ) contract. Individual Task Orders (TOs) shall be issued on a Firm Fixed Price (FFP) basis.

The Contractor shall provide and/or acquire the services, hardware, and software required by individual TOs, consistent with the general requirements of this PWS.

## 4.1 PERFORMANCE PERIOD:

The Ordering Period shall be four (4) years from the date of award. The period of performance (PoP) for any TO may go up to 12 months beyond the last day of the Ordering Period. Each TO will have its own PoP.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are eleven (11) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

| | |
|---|---|
| New Year's Day | January 1 |
| Juneteenth | June 19 |
| Independence Day | July 4 |
| Veterans Day | November 11 |
| Christmas Day | December 25 |

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

| | |
|---|---|
| Martin Luther King's Birthday | Third Monday in January |
| Washington's Birthday | Third Monday in February |
| Memorial Day | Last Monday in May |
| Labor Day | First Monday in September |
| Columbus Day | Second Monday in October |
| Thanksgiving | Fourth Thursday in November |

**4.2 PLACE OF PERFORMANCE:**

The place of performance shall be identified in individual TOs within our HCS(s). The list of current Health Care Systems supported this by this requirement, and their addresses, are given in Table 1.

| ID | Name | Address | PEW System in Use |
|---|---|---|---|
| 570 | Central California Health Care System (CCHCS) | 2615 E. Clinton Ave. Fresno, CA 93703-2286 | None |
| 612 | Northern California Health Care System (NNHCS) | 10535 Hospital Way Mather, CA 95655 | Securitas WanderGuard |
| 640 | Palo Alto Health Care System (PAHCS) | 3801 Miranda Ave. Palo Alto, CA 94304 | CenTrak Wander Management |

| | | | |
|---|---|---|---|
| 654 | Sierra Nevada Health Care System (SNHCS) | 975 Kirman Avenue Reno, NV 89502 | Accutech ResidentGuard |
| 662 | San Francisco Health Care System (SFHCS) | 4150 Clement St. San Francisco, CA 94121 | Securitas WanderGuard |
| 593 | North Las Vegas Health Care System (NLVHCS) | 6900 N. Pecos Road Las Vegas, NV 89086 | CenTrak Wander Management |
| 459 | Pacific Islands Health Care System (PIHCS) | 459 Patterson Road Honolulu, HI 96819 | Securitas WanderGuard |

**Table 1: Health Care Systems covered under the scope of this contract**

### 4.2.1 TRAVEL:

The Government anticipates travel under this effort to perform the tasks associated with the effort. Travel costs are included in the firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program related meetings for this effort will be dependent on each TO.

## 5.0 SPECIFIC TASKS AND DELIVERABLES:

Individual TOs may cover multiple functional areas outlined below. These functional area descriptions are provided to offer greater insight into the complexity and uniqueness of potential TO requirements addressed in this Performance Work Statement (PWS). Functional areas are not mutually exclusive; a single TO may include requirements spanning several areas.

### 5.1 TECHNOLOGY AND PROJECT MANAGEMENT:

The Contractor shall implement comprehensive technology and project management practices across all TOs. Responsibilities include developing and maintaining a Master Project Plan (MPP) covering scope, schedule, cost, quality, resources, communications, risks, and delivery, as well as; coordinating multi-disciplinary stakeholders (Nursing, Healthcare Technology Management (HTM), Office of Information Technology (OIT), Supply Chain Management (SCM), Engineering, etc.). The Contractor shall administer formal governance routines (steering committee, change control board) and maintain artifacts (risk/issue/change logs) in a VA-approved repository. The Contractor shall assist with defining, tracking, and continuously refining KPIs aligned to VA objectives including location accuracy, system uptime, and integration success rate, with variance analysis and corrective action plans. Project controls shall include dependency tracking and critical path analysis.

**Deliverables:**

- **Master Project Plan (MPP)** – Microsoft PowerPoint or PDF, baseline within 30 days of TO award; updated monthly; includes milestones, dependencies, resource plan, and critical path; accepted when dates/logic are consistent and achievable.

- **Stakeholder Engagement Plan** - PDF; due within 30 days; meeting cadences, roles/RACI, communications channels, escalation paths; accepted when all VA stakeholder groups are identified and engagement commitments scheduled.

- **Risk, Issue, and Change Logs** - Living spreadsheet or IT service agreement (ITSM) tool export; updated weekly; include probability/impact, owners, target dates, and mitigations; accepted when items have owners and dated actions.

- **Status Reports (Monthly)** - PDF, MS PowerPoint, or dashboard; schedule performance index (SPI), KPIs, accomplishments/next steps, risks/issues; accepted when variances >±10% include corrective actions.

- **KPI Dashboard** - Power BI; refreshed at least weekly; displays system uptime, accuracy, retrieval time, interface error rates; accepted when data sources are validated and thresholds codified.

### 5.1.1 SYSTEM DESIGN AND ARCHITECTURE:

The Contractor shall lead structured discovery activities—including interviews, workshops, and site assessments—to capture clinical workflows, patient movement patterns, staff response requirements, and compliance constraints related to elopement prevention. The Contractor shall conduct design reviews with VA stakeholders and document all decisions and resolutions. Using these inputs, the Contractor shall produce an end-to-end architecture for the PEW prevention platform, including:

- Coverage designs for zonal, room-level, and exit-point accuracy
- Geofencing strategies for restricted areas
- Capacity plans for tag and device density
- Data models for patient profiles, alarm states, and location hierarchies

Designs shall specify:

- Accuracy targets (≥99%)
- Redundancy and failover strategies
- Network and security baselines
- Interoperability with VA enterprise systems (e.g., nurse call, access control, fire alarms)

### 5.1.2 HARDWARE AND SERVER DESIGN DOCUMENTATION:

The Contractor shall develop and maintain a hardware and server design document for each site, updating it throughout implementation to reflect current design. The design document shall include:

- Proposed changes to VA-provided maps and Engineering Space Files
- Hardware installation locations for monitors, chokepoints, and exit controllers
- Draft server configuration and architecture optimized for facility needs, including:
    - Diagrams detailing server requirements
    - Expected WAN bandwidth utilization
    - Application latency considerations
    - Server specifications (power, thermal outputs, network connections)
    - Supported number of patient tags per server

The Contractor shall ensure all applications synchronize with internal VA site time standard. The synchronization of time on this network is critical in every aspect of managing, securing, planning, and debugging as it involves determining when an event occurred.

**Deliverables:**

- **Requirements Specification** — PDF; due within 45 days; use-case narratives, non-functional requirements, constraints; accepted when traced to design and test cases.

- **System Architecture Diagram** — PDF; due within 60 days; logical/physical views, interfaces, data flows, security zones; accepted after VA review sign-off.

- **Coverage Maps & Accuracy Models** — Floor plans with reader/beacon placements; propagation models; accepted when modeled accuracy meets targets by area.

- **Design Review Report** — PDF; per review; comments, decisions, action items; accepted when all critical actions have owners and due dates.

### 5.1.3 HARDWARE PROVISIONING:

The Contractor shall provide all required hardware components to implement and expand a PEW system. Hardware is ordered at the Task Order level. Wireless hardware shall meet FIPS-compliant security standards.

The Contractor shall coordinate delivery schedules with VA stakeholders and obtain written or email concurrence from the Contracting Officer's Representative (COR) prior to shipment. Upon delivery, the Contractor shall provide the COR with a signed Facility Receiving Report for each site, confirming the order and delivery of components,

reconciling any discrepancies, and detailing delivery time, location, and the Government representative who received the shipment.

**Categories Of Hardware to Be Provided**

- **System Components:** include but not limited to patient protection tags, exit controllers for doors and elevators, low-frequency (LF) chokepoints for egress detection, patient safety bands with tamper/cut detection, location readers, gateways, and supporting infrastructure.

- **Networking and Infrastructure:** Cabling and any supplemental wireless hardware required for connectivity (FIPS-compliant).

- **Server and Storage Hardware:** As specified in the Hardware and Server Design Document (HSDD) for local or centralized processing, including capacity for real-time alerting and reporting.

### 5.1.4 SOFTWARE PROVISIONING:

The Contractor shall provide all required software components required for PEW prevention for each site as specified and ordered at the Task Order level. The Contractor shall ensure that all software licenses are valid for the entire period of performance (PoP) and include rights for installation, configuration, integration, and ongoing support. All software shall meet VA cybersecurity requirements, including FIPS-compliant encryption and adherence to VA Handbook 6500 standards.

The Contractor shall coordinate with VA stakeholders to schedule software delivery and installation and obtain written or email concurrence from the Contracting Officer's Representative (COR) prior to deployment. Upon installation, the Contractor shall provide the COR with a signed Software Provisioning Report for each site, confirming delivery, installation, and configuration details, as well as reconciliation of any discrepancies between planned and actual deployment.

**CATEGORIES OF SOFTWARE TO BE PROVIDED:**

- **Application**: patient protection platform, location engine, alert management, and device administration tools, and configuration tools for exit controllers and patient tags (if applicable).

- **Integration Software**: Connectors and APIs for interoperability with VA enterprise systems (e.g., nurse call, access control, fire alarms).

- **Supporting Software**: Database components, reporting modules, and analytics tools for alarm history, compliance tracking, and performance dashboards.

### 5.1.5 STAGING:

The Contractor shall manage delivery of approved hardware/software and accessories, preparing a detailed Bill of Materials (BoM) and delivery schedule aligned to installation waves. Staging shall include firmware standardization, configuration pre-loads, and quality checks. Interoperability validation (firmware compatibility, protocol settings) shall be performed prior to shipment to sites. The Contractor shall document serials, MACs, tag IDs, and association procedures to enable traceability.

**Deliverables:**

- **Delivery Schedule** — PDF or PowerPoint view; delivery windows, critical dependencies; accepted when aligned to installation plan.

- **Pre-Configuration Checklist** — PDF; per batch; firmware versions, network settings, tag profiles; accepted when spot-checked devices meet baselines.

- **Inventory & Serial Log** — Spreadsheet; ongoing; serials/MACs/tag IDs, location, status; accepted when entries reconcile with shipment records.

### 5.1.6 HARDWARE INSTALLATION AND CONFIGURATION:

The Contractor shall perform complete installation and configuration of all hardware and software components as specified in the TOs. The Contractor shall ensure that all hardware installation and software configuration are performed strictly in accordance with the Original Equipment Manufacturer (OEM) standards and guidelines. This includes adherence to OEM and VA specifications for mounting, power, network connectivity, calibration, firmware versions, and software setup. The Contractor shall document compliance with these standards in the installation and configuration reports and provide evidence of OEM-approved methods for any deviations. Failure to meet manufacturer standards may result in rejection of work and require corrective action at no additional cost to the Government. Specific tasks include:

**PRE-INSTALLATION PREPARATION:**

- Site Assessment — Conduct walkthroughs to identify installation points for readers, exciters, gateways, and beacons; validate power and network availability; and update facility maps with proposed hardware placement.

- Hardware Staging — Verify firmware versions for all devices, pre-configure network settings, and label/inventory all components.

**PHYSICAL INSTALLATION:**

- Mounting Readers — Install ceiling or wall-mounted readers at designated coverage zones, ensuring proper orientation, height, connect to network infrastructure, calibrate read ranges, and validate tag detection performance.

- Installing Exciters — Place exciters at room entry points for room-level accuracy, configure zone IDs and power levels, and test proximity detection for tag activation.

- Gateway Deployment — Install gateways to aggregate data, validate network connectivity, and configure failover and redundancy settings.

- BLE Beacon Placement — Deploy BLE beacons strategically for optimal coverage and accuracy, mount securely, and calibrate signal strength for room-level precision.

The Contractor shall coordinate installation schedules with VA stakeholders, minimize clinical disruption, and provide written confirmation of completion.

### 5.1.7 SOFTWARE INSTALLATION AND CONFIGURATION:

Software configuration shall include deployment of PEW patient protection applications, along with any required integration components for alerting, reporting, and interoperability with VA enterprise systems. All installations shall comply with VA cybersecurity requirements, including FIPS-compliant encryption, and shall be documented with as-built diagrams and configuration baselines. In response to hardware design changes or VA reconfiguration requirements, the Contractor shall update rendered maps and zone configurations within the user interface (UI). Configuration changes shall be defined during the site assessment at each facility.

**PRE-INSTALLATION PREPARATION:**

- Software Licensing and Validation**:** Verify valid licenses for application software; ensure compliance with VA cybersecurity and FIPS requirements.

- Environment Readiness: Confirm server specifications, network connectivity, and database availability for hosting applications; validate compatibility with VA standard configurations (Windows® 10, Edge, etc.).

**SOFTWARE INSTALLATION:**

- Install PEW applications: Deploy location engine and alert management modules; configure device communication and event processing, configure integration with exit controllers and patient tags.

- Deploy UI Components: Install web-based or server-hosted UI for monitoring and alarm management; ensure HTTPS and secure authentication mechanisms are enabled.

**CONFIGURATION:**

- Software Configuration: Define patient profiles, alarm rules, and location hierarchies; calibrate IR and LF chokepoints for accurate egress detection, dashboards, alert routing, and geofencing zones; set up per-patient security profiles and transport overrides.

- Integration Configuration: Enable interoperability with VA systems (e.g., nurse call, access control, fire alarms); configure APIs and connectors for real-time data exchange.

- UI Configuration: Configure map views, alarm filters, and reporting templates; enable Power BI integration for analytics.

**INTEGRATION:**

- Data Synchronization: Validate interoperability between the PEW application and VA enterprise systems; ensure consistent alarm and location updates across platforms.

- API and Connector Setup: Configure secure APIs for real-time data exchange; test authentication and data integrity.

**TESTING AND VALIDATION:**

- Functional Testing: Verify UI features such as map rendering, alarm notifications, and reporting; confirm dashboards display accurate patient location and event data.

- Performance Testing: Validate system response times, data refresh intervals, and failover mechanisms.

### 5.1.8 USER INTERFACE PROVISIONING AND CONFIGURATION:

The proposed User Interface (UI) shall be a secure platform that provides comprehensive patient location monitoring and alarm management capabilities for elopement prevention. The Contractor shall integrate the UI with VA enterprise systems, including nurse call, access control, and fire alarm systems, and validate interoperability across all technologies. At a minimum, the UI must allow users to view individual patient details—including tag ID, location, and alarm status—display facility layouts in both map and list views with search functionality by patient name or tag ID, and configure alarm rules for unauthorized egress, tamper detection, and transport overrides. The UI shall support exporting alarm and event data in Excel format, implementing customizable business rules, generating real-time alerts for elopement events, and producing reporting dashboards integrated with Microsoft® Power BI for analytics and performance metrics. Additionally, the UI must allow user-configurable refresh intervals, accurately reflect space changes and patient status updates, and stop sending location updates for discharged or deactivated patients.

### 5.1.9 SYSTEM ADMINISTRATION:

The Contractor shall provide Database and System Administration services during implementation and the warranty period, including periodic health checks on servers and databases, monitoring application logs, ensuring security compliance and remediation of vulnerabilities, applying monthly OS security patches from VA OIT, troubleshooting connectivity and server/application startup issues, and implementing software updates and upgrades.

### 5.1.10 PROFESSIONAL SERVICES HOURS:

The Contractor shall provide service hours as requested by the Government for tasks including system and software configuration and administration, ensuring hardware and software compliance with VA standards, implementing workflow solutions, project planning and management, and delivering analytics and business intelligence.

## 5.2 Acceptance testing:

The Contractor shall develop an **Acceptance Test Plan** for each TO and obtain VA approval prior to execution. Testing will occur in two phases.

### 5.2.1 PHASE 1: PERFORMANCE TESTING

The Contractor shall validate system functionality and confirm room-level location accuracy of at least **99%**. Testing must ensure compliance with all specifications and verify that no interference occurs with other facility devices. The Contractor shall provide VA with the performance test methodology and results. If the system does not meet requirements, the Contractor shall submit a **Facility Remediation Hardware Report** detailing additional hardware, software, or services needed. A **Final Hardware Deployment Document** shall also be provided, listing all installed hardware with unique identifiers and exact locations.

### 5.2.2 PHASE 2: USER ACCEPTANCE TESTING

The Contractor shall schedule user acceptance testing with **30 days' notice** and provide qualified personnel to assist VA during the process. The COR shall be responsible for the test methodology, and the Contractor shall deliver the results. A **Facility Acceptance Test Report** shall be submitted in Excel format, showing tag IDs, locations, and whether accuracy requirements were met.

**Deliverables:**

- **Performance Test Plan & Results** - PDF; includes test steps, accuracy verification, and interference checks; accepted when results meet ≥95% of the requirements.

- **Facility Remediation Hardware Report** - PDF; lists additional hardware/software/services required for compliance; accepted when all remediation items are documented.

- **Final Hardware Deployment Document** - PDF and Excel; floor map layout and table of installed hardware with IDs and locations; accepted when reconciled with design documents.

- **User Acceptance Test (UAT) Plan** - PDF; outlines UAT process, roles, and schedule; accepted when approved by VA and Contractor before testing.

- **Facility Acceptance Test Report** - Excel; provides tag IDs, locations, and accuracy ratings; accepted when accuracy metrics are clearly reported and validated.

### 5.2.3 TRANSITION PLANNING:

The Contractor shall prepare a comprehensive Transition Plan to transfer all operational responsibilities for patient elopement prevention systems to VA staff by the end of the contract. The plan must include detailed procedures for hardware management, software configuration, ongoing maintenance, and system administration, organized in a RACI matrix to clearly define roles and responsibilities. The Contractor shall execute the approved transition plan and provide complete User and Technical Manuals for all PEW system components, including troubleshooting guides, diagnostic tools, and parts lists. Each facility shall receive two copies of operator manuals and two copies of technical service manuals to ensure continuity of operations and support after contract completion.

**Deliverables:**

- **Transition Plan** — PDF; details step-by-step transition procedures and RACI matrix; accepted when reviewed and approved by VA.

- **User and Technical Manuals** — PDF; includes operating instructions, troubleshooting guides, and parts lists; accepted when complete and facility-specific.

### 5.2.4 TRAINING REQUIREMENTS:

The Contractor shall develop a comprehensive Training Plan and deliver on-site or remote sessions for both technical and non-technical users, including nursing staff, Behavioral Health clinicians, Biomedical Engineering personnel, security teams, and system administrators. The Training Plan must outline schedules, delivery methods, audience profiles, and instructor qualifications. Training shall cover system operation, alarm response workflows, patient tag management, and troubleshooting procedures to ensure staff can effectively prevent and respond to elopement events. Each session shall be documented with attendee lists and completed according to the approved plan, ensuring compliance with VA standards and readiness for go-live.

**Deliverables:**

- **Training Plan** — PDF; outlines training objectives, schedule, and delivery method; accepted when approved by VA.
- **Training Material and Schedules** — PDF; includes content and timing for each session; accepted when aligned with the Training Plan.
- **List of Attendees** — Excel or PDF; records participants and trainer details; accepted when complete and facility-specific.

#### 5.2.5 WARRANTY SERVICES:

All hardware, software, and services provided under this contract shall include a one-year manufacturer's warranty covering parts, labor, and technical support for PEW prevention systems. During the warranty period, the Contractor shall provide maintenance and technical assistance, oversee any subcontractor support, and offer extended warranty options upon VA request. The Contractor shall maintain and submit a Warranty Status Report detailing all system components, specifications, and warranty expiration dates. Additionally, the Contractor shall ensure help desk support responds within two hours of initial contact and that any required on-site service is completed within 10 business days to minimize disruption to patient safety operations.

**Deliverable:**

- **Warranty Status Report** — PDF; lists hardware/software specifications and warranty expiration dates; accepted when accurate and reconciled with deployment records.

## 6.0 GENERAL REQUIREMENTS

### 6.1 ENTERPRISE AND IT FRAMEWORK

#### 6.1.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (VA TRM). The VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a technology roadmap and tool for supporting OIT. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

#### 6.1.2 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.

### 6.1.3 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), https://www.ea.oit.va.gov/EAOIT/VA_EA/Enterprise_Technical_Architecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, https://www.oit.va.gov/library/recurring/edp/index.cfm. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements 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 card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-05-24, M-19-17, and NIST Federal

Information Processing Standard (FIPS) 201-2. OMB Memoranda M-05-24 and M-19-17 can be found at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf, and https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's Master Person Index (MPI) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion-based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-4 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896.

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

### 6.1.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support Internet Protocol Version 6 (IPv6) 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). IPv6 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 shall support native IPv6 and 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 and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and dual stack (IPv6 / IPv4) operations.

### 6.1.5 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). Any deviations must be approved by the VA TIC 3.0 Working Group at vaoisesatic30team@va.gov.

### 6.1.6 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 10 (64bit), Edge (Chromium based), and 365 Apps for enterprise. Applications delivered to VA and intended to be deployed to Windows 10 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using Microsoft Endpoint Configuration Manager (CM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

### 6.1.7 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM)

The Contractor shall support VA efforts IAW the Veteran-Focused Integration Process (VIP) Guide and Product Line Management (PLM) Playbook. The major focus of VIP is

on Enterprise Oversight, Governance, reporting, and establishing practices that focus on outcomes and continuously delivering sustainable IT capabilities to benefit the Veteran. PLM is a framework that focuses on delivering functional products that provide the highest priority work to customers while delivering simplified, reliable, and practical solutions to the business, medical staff, and our Veterans. The VIP Guide is a companion guide to the PLM Transformation Playbook and can be found at: https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371 and the PLM Transformation Playbook can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

The VIP Guide provides guidance for transitioning from project-centric to product-centric delivery. The VIP guide applies to all OIT Office of Management and Budget (OMB) reportable products that are required to collect and report costs, schedules, risks, and other valuable information in VA PARS (whether products are procured or developed by VA) and any VA Information Technology project effort in Software Product Management (SPM) and Infrastructure Operations (IO), or their successors, that touch the VA network regardless of IT organizational alignment (whether it spends government funding from VA's Congressional IT Appropriation or any other appropriation).

The PLM Transformation Playbook details how OIT leadership expects Product Lines (PLs) to implement PLM, DevOps, and Lean-Agile principles, methods, practices, and techniques through levels of maturity. The PLM Transformation Playbook applies to all Information Technology (IT) products aligned to PLs in the Software Product Management, Infrastructure Operations and Product Engineering organizations within the OIT organization.

Others outside the referenced groups or organizations may use the VIP Guide and PLM Transformation Playbook for situational awareness as needed.

### 6.1.8 PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf. The main PAL can be accessed at www.va.gov/process.

### 6.1.9 AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall EA that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department's Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below. The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA's Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with VA Profile to access personal contact information, if the solution relies on VA Veteran personal contact information data. VA Profile is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active-duty military service data. VADIR is the authoritative source for qualifying active-duty military service in VA.
7. Interfacing with VA Systems Inventory (VASI) to access VA systems information, if the solution relies on VA system information. VASI is the authoritative source for VA Information Technology systems.
8. Interfacing with Enterprise Mission Assurance Support Service (eMASS) to access the historical Authority to Operate (ATO) status of all VA Information Systems prior to migrating to ServiceNow Continuous Authorization and Monitoring (SNowCAM) until it is determined the migration is completed and eMASS is sunset. eMASS contains the historical Authority to Operate (ATO) status of all VA Information Systems prior to September 30, 2025, with all status provided through SNowCAM once migration is completed.

### 6.1.10 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 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.

### 6.1.11 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.

### 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

**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

**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

## 6.2 SECURITY AND PRIVACY REQUIREMENTS

### 6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

| **Position Sensitivity** | **Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A) |
|---|---|
| **Low / Tier 1** | **Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions. |
| **Moderate / Tier 2** | **Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree. |
| **High / Tier 4** | **Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree. |

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

Position Sensitivity and Background Investigation Requirements by Task

| **Task Number** | **Tier1 / Low / NACI** | **Tier 2 / Moderate / MBI** | **Tier 4 / High / BI** |
|---|---|---|---|
| 5.0 | ☒ | ☐ | ☐ |

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will

be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

### 6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints
f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM)

Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

**Deliverable:**

A. Contractor Staff Roster

## 6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access

2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

### 6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

| Performance Objective | Performance Standard | Acceptable Performance Levels |
|---|---|---|
| A. Technical Needs | 1. Demonstrates understanding of requirements<br>2. Efficient and effective in meeting requirements<br>3. Meets technical needs and mission requirements<br>4. Offers quality services/products | Satisfactory or higher |
| B. Project Milestones and Schedule | 1. Established milestones and project dates are met<br>2. Products completed, reviewed, delivered in timely manner<br>3. Notifies customer in advance of potential problems | Satisfactory or higher |
| C. Project Staffing | 1. Currency of expertise<br>2. Personnel possess necessary knowledge, skills and abilities to perform tasks | Satisfactory or higher |
| D. Value Added | 1. Provided valuable service to Government<br>2. Services/products delivered were of desired quality | Satisfactory or higher |

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

## 6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a

significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

**6.6 GOVERNMENT FURNISHED PROPERTY: None**

**6.7 SHIPMENT OF HARDWARE OR EQUIPMENT**

**Shipping Address / Mark For requirements:**

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

**Ship To and Mark For: (To be identified at TO Level)**

| | Primary | | Alternate |
|---|---|---|---|
| Name: | _____ | Name: | _____ |
| Address: | _____ | Address: | _____ |
| Voice: | _____ | Voice: | _____ |
| Email: | _____ | Email: | _____ |

**Special Shipping Instructions:**

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of hardware to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

**Packing Slips/Labels and Lists shall also include the following:**

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: (e.g. Tier I Lifecycle Refresh)

Total number of Containers: Package ___ of ___. (e.g., Package 1 of 3)

Shipment/Delivery Kick-off Meeting

The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the VA Program Manager (PM), COR, Delivery Date Coordinator, Implementation Manager, and Facility CIOs (or designee) to discuss delivery schedule requirements and facilitate delivery of equipment. This meeting may be held in conjunction with the post award conference or identified technical kickoff meeting. The Contractor shall also present the Shipment/Delivery Weekly Progress Report format for review and approval by the Government. This meeting, if held independently, shall be conducted telephonically within ten days after award and shall incorporate any delivery schedule changes to the draft Delivery Schedule identified by the Government.

Shipment/Delivery Weekly Progress Report

The Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify the items shipped, the serial number associated with each piece of equipment; the date of each shipment; the status of each shipment, tracking information, and information relative to Government-receipt of the equipment items at each delivery site. In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems and provide a description of how the problems were resolved/addressed. If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution. Shipment/Delivery Weekly Progress Reports shall be submitted in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

Deliverables:

A. Master Delivery Schedule

B. Shipment/Delivery Weekly Progress Report

# ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

## A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

## A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

### **A2.1.** VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the

Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

### A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

### A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self contained, closed products
- ☒ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

### A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

### A3.3. Compatibility with Assistive Technology

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

### A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

**Deliverables:**

A. Final Section 508 Compliance Test Results

### A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.

3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

### A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained

during the performance this contract, the Contractor has a responsibility to ask the VA CO.

5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
   a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
   b. Controlled access to system and security software and documentation.
   c. Recording, monitoring, and control of passwords and privileges.
   d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
   e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
   f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
   g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
   h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

## A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic

Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

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

## APPLICABLE PARAGRAPHS TAILORED FROM: THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

### B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

### B2. 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, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative 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 must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

## B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

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

11. Notwithstanding the provision above, the Contractor/Subcontractor 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 health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the

Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

## B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program and theTIC Reference Architecture*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

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

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods.

This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**, but in no event longer than 7 days.**

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes **within 7 days*.***

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

## B5. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. 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 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.

## B6. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

    a) date of occurrence;
    b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
3) Number of individuals affected or potentially affected;
4) Names of individuals or groups affected or potentially affected;
5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
6) Amount of time the data has been out of VA control;
7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;
9) Assessment of the potential harm to the affected individuals;
10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

## B7. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

## B8. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176)

understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix D relating to access to VA information and information systems.

2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, 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 training and documents are complete.

## B.5 CONTRACT MAXIMUM/MINIMUM

In accordance with Section C, clause RFO 52.216-22 entitled, “Indefinite Quantity” the maximum value of the VISN 21 Automated Asset Management Using Passive Radiofrequency Identification and Bluetooth Low Energy Hardware, Software, and Professional Services contract is $TBD. The cumulative value of all Task Orders issued under this contract shall not exceed the maximum amount.

In accordance with Section C, clause RFO 52.216-22 entitled, “Indefinite Quantity” the Minimum guaranteed value under the VISN 21 Automated Asset Management Using Passive Radiofrequency Identification and Bluetooth Low Energy Hardware, Software, and Professional Services contract is $10,000.00 and shall be met through the issuance of the first delivery order.

## B.6 ORDERING PROCEDURES

a. Orders against this contract will be issued at the sole discretion of the Government by a VA Contracting Officer during the period of the award date through 48 months thereafter. Upon receipt of a Task Order, the contractor shall provide the supplies and services at the prices set forth in the schedule above.

b. Orders may be issued only as Firm Fixed Price. Each order is a stand-alone order. To place an order, the Contracting Officer will issue a SF1449 that will include the specific products or services required by VA as defined in the base contract. The contractor will not be required to submit a quote. If the contractor cannot accept the order, it must inform the Contracting Officer within two business days of receipt of order and must propose a new date of performance. Regardless of the actual delivery date of equipment, performance of services, or the period of performance for maintenance, the pricing shall remain the same as the ordering period the Task Order was issued in.

## SECTION C - CONTRACT CLAUSES

### C.1 RFO 52.212-4 CONTRACT TERMS AND CONDITIONS -- COMMERCIAL ITEMS (Deviation Date: October 28, 2025)

### ADDENDUM to RFO 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (Deviation Date: October 28, 2025)

The following clauses are incorporated into 52.212-4 as an addendum to this contract:

### RFO 52.252-2 CLAUSES INCORPORATED BY REFERENCE (DEVIATION OCT 2025)

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/far-overhaul/far-part-deviation-guide/far-overhaul-part-52#FAR_52_252_2 (RFO)

http://www.va.gov/oal/library/vaar/index.asp (VAAR)

(End of Clause)

| RFO/VAAR NUMBER | TITLE | DATE |
|---|---|---|
| 52.203-6 | RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT | JUN 2020 |
| 52.203-12 | PREVENTING PERSONAL CONFLICTS OF INTEREST | JUN 2020 |
| 52.203-16 | PREVENTING PERSONAL CONFLICTS OF INTEREST | JUN 2020 |
| 52.203-17 | CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS | JUN 2020 |
| 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 |
| 52.204-10 | REPORTING EXECUTIVE COMPENSATION & FIRST-TIER SUBCONTRACT AWARDS | DEVIATION OCT 2025) |
| 52.204-13 | SYSTEM FOR AWARD MANAGEMENT MAINTENANCE | DEVIATION OCT 2025) |

| RFO/VAAR NUMBER | TITLE | DATE |
|---|---|---|
| 52.209-6 | PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED | DEVIATION OCT 2025) |
| 52.209-9 | UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS | JAN 2025 |
| 52.209-10 | PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS | DEVIATION OCT 2025) |
| 52.219-8 | UTILIZATION OF SMALL BUSINESS CONCERNS | DEVIATION OCT 2025) |
| 52.219-13 | NOTICE OF SET-ASIDE OF ORDERS | MAR 2020 |
| 52.219-14 | LIMITATIONS ON SUBCONTRACTING | DEVIATION OCT 2025) |
| 52.219-27 | NOTICE OF SDVOSB SET ASIDE | OCT 2022 |
| 52.219-28 | POSTAWARD SMALL BUSINESS PROGRAM REREPRESENTATION | DEVIATION OCT 2025) |
| 52.222-3 | CONVICT LABOR | DEVIATION OCT 2025) |
| 52.222-35 | EQUAL OPPORTUNITY FOR VETERANS | DEVIATION OCT 2025) |
| 52.222-36 | EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES | DEVIATION OCT 2025) |
| 52.222-37 | EMPLOYMENT REPORTS ON VETERANS | DEVIATION OCT 2025) |
| 52.222-40 | NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT | DEVIATION OCT 2025) |
| 52.222-50 | COMBATING TRAFFICKING IN PERSONS | DEVIATION OCT 2025) |
| 52.222-54 | EMPLOYMENT ELIGIBILITY VERIFICATION | DEVIATION OCT 2025) |
| 52.224-3 | PRIVACY TRAINING | JAN 2017 |
| 52.225-1 | BUY AMERICAN--SUPPLIES | DEVIATION OCT 2025 |
| 52.225-3 | BUY AMERICAN--FREE TRADE AGREEMENTS--ISRAELI TRADE ACT | DEVIATION OCT 2025 |
| 52.225-5 | TRADE AGREEMENTS | NOV 2023 |

| RFO/VAAR NUMBER | TITLE | DATE |
|---|---|---|
| 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 | NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT | JUN 2020 |
| 52.227-16 | ADDITIONAL DATA REQUIREMENTS | JUN 1987 |
| 52.227-17 | RIGHTS IN DATA-SPECIAL WORKS | |
| 52.228-5 | INSURANCE-WORK ON A GOVERNMENT INSTALLATION | JAN 1997 |
| 52.232-33 | PAYMENT BY ELECTRONIC FUNDS TRANSFER - 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 |
| 52.233-4 | APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM | DEVIATION OCT 2025 |
| 52.237-2 | PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, VEGETATION | APR 1984 |
| 52.237-3 | CONTINUITY OF SERVICES | JAN 1991 |
| 52.242-13 | BANKRUPTCY | JUL 1995 |

(End of clause)

**RFO 52.216-18 ORDERING (AUG 2020)**

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from: the information will be entered at award (The ordering period shall be four (4) years from the date of award).

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) A delivery order or task order is considered "issued" when—

(1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;

(2) If sent by fax, the Government transmits the order to the Contractor's fax number; or

(3) If sent electronically, the Government either—

(i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or

(ii) Distributes the delivery order or task order via email to the Contractor's email address.

(d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

(End of clause)

**RFO 52.216-19 ORDER LIMITATIONS (OCT 1995)**

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $3,500, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor—

(1) Any order for a single item in excess of $500,000.00;

(2) Any order for a combination of items in excess of $1,000,000.00 or

(3) A series of orders from the same ordering office within 10 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 3 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

**RFO 52.216-22 INDEFINITE QUANTITY (OCT 1995)**

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 60 months and shall complete all current deliveries or installation within a year after contract expiration. This does not include warranties and/or maintenance, whose terms may extend beyond a year days of contract expiration as determined by individual task order and delivery terms.

(End of Clause)

**RFO 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)

**VAAR 852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 2022)**

The Contracting Officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation letter shall be furnished to the Contractor.

(End of clause)

**VAAR 852.203-70 COMMERCIAL ADVERTISING (MAY 2018)**

The Contractor shall not make reference in its commercial advertising to Department of Veterans Affairs contracts in a manner that states or implies the Department of Veterans Affairs approves or endorses the Contractor's products or services or considers the Contractor's products or services superior to other products or services.

(End of Clause)

**VAAR 852.212-71, GRAY MARKET AND COUNTERFEIT ITEMS (FEB 2023)**

(a) No used, refurbished, or remanufactured supplies or equipment/parts shall be provided. This procurement is for new Original Equipment Manufacturer (OEM) items

only. No gray market items shall be provided. Gray market items are OEM goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

(b) No counterfeit supplies or equipment/parts shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

(c) Vendor shall be an OEM, authorized dealer, authorized distributor, or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

(End of clause)

**VAAR 852.204-70 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (MAY 2020)**

(a) The Contractor shall comply with current Department of Veterans Affairs policy for personal identity verification of all employees performing under this contract when frequent and continuing access to VA facilities or information systems is required.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor's employees will require frequent and continuing access to VA facilities or information systems.

(End of clause)

**VAAR 852.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2023)**

(a) Definitions. As used in this clause—

Business Associate means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another covered entity, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, that performs or assists in the performance of a function or activity on behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI). The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the Privacy Rule, between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

Information technology (see RFO 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts which include services (including support services), and related resources for information technology as defined in 802.101.

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual's identity, including but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records.

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and

information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

(b) General. Contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(c) Access to VA information and VA information systems. (1) Contractors are limited in their request for logical or physical access to VA information or VA information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with VA information are subject to the same investigative 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 to access VA information and VA information systems shall be in accordance with VA Directive and Handbook 0710, Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) HIPAA Business Associate Agreement requirement. Contractors shall enter into a Business Associate Agreement (BAA) with VHA, VA's Covered Entity, when contract requirements and access to protected health information is required and when requested by the Contracting Officer, or the Contracting Officer's Representative (COR) (see VAAR 824.103-70). Under the HIPAA Privacy and Security Rules, a Covered

Entity (VHA) must have a satisfactory assurance that its PHI will be safeguarded from misuse. To do so, a Covered Entity enters into a BAA with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's PHI for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same disclosure restrictions to PHI that is required of the Covered Entity in situations where a contractor—

(i) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the Covered Entity; or

(ii) Provides one or more of the services specified in the Privacy Rule to or for the Covered Entity.

(A) Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates. BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA. There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(B) BAA requirement flow down to subcontractors. A prime Contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the Contractor. Contractors employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the Covered Entity and the prime Contractor.

(d) Contractor operations required to be in United States. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other VA policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable Business

Associate Agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information Technology Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) Contractor/subcontractor employee reassignment and termination notification. Contractors and subcontractors shall provide written notification to the Contracting Officer and Contracting Officer's Representative (COR) immediately, and not later than four (4) hours, when an employee working on a VA information system or with access to VA information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant VA contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(f) VA information custodial requirements. (1) Release, publication, and use of data. Information made available to a Contractor or subcontractor by VA for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without VA's prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in Rights in Data—General, RFO 52.227-14(d).

(2) Media sanitization. VA information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and VA requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see VA Directive 6500, VA Cybersecurity Program).VA reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and VA requirements. The Contractor and subcontractor will provide all necessary access and support to VA and/or GAO staff during periodic control assessments or audits.

(3) Data retention, destruction, and contractor self-certification. The Contactor and its subcontractors are responsible for collecting and destroying any VA data provided, created, or stored under the terms of this contract, to a point where VA data or materials are no longer readable or reconstructable to any degree, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, or subsequent issue. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction of all VA data in its possession according to VA Directive 6500, and VA Cybersecurity Program, including compliance with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) Return of VA data and information. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VA (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying BAA. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract using VA-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or equipment will be destroyed unless done in accordance with the terms of this contract and the VHA Records Control Schedule 10-1.

(5) Use of VA data and information. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies.If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if the National NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) Copying VA data or information. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) Violation of information custodial requirements. If VA determines that the Contractor has violated any of VA’s information confidentiality, privacy, or security provisions, it shall be sufficient grounds for VA to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with RFO part 49 or terminate for cause in accordance with RFO 12.403.

(8) Encryption. The Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract, using cryptography, and VA-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) Firewall and web services security controls. The Contractor/subcontractor's firewall and web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

(10) Disclosure of VA data and information. Except for uses and disclosures of VA information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose VA information only in two other situations: (i) subject to paragraph (f)(10) of this section, in response to a court order from a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose VA information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of VHA, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated VA facility Privacy Officer as provided in the contract, BAA, or by the Contracting Officer. If providing the Accounting of Disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose VA information protected by any of VA’s privacy statutes or applicable regulations including but not limited to: the Privacy Act of 1974, 38 U.S.C. 5701, confidential nature of claims, 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus or the HIPAA Privacy Rule. If the Contractor/subcontractor is in receipt of a court order or other requests for VA information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(g) Report of known or suspected security/privacy incident. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR or within one (1) hour of an incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. See VA Data Breach Response Service at https://www.oprm.va.gov/dbrs/about_dbrs.aspx. Report all actual or suspected security/privacy incidents and report the information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than 7 days.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within 14 days.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, but within 60 days of discovery or disclosure. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of VA) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology. These exceptions will be tracked by the Contractor in concert with the Government in accordance with VA Directive 6500 and related VA Handbooks.

(h) Security and privacy incident investigation. (1) The term “privacy incident” means the unauthorized disclosure or use of VA information protected under a confidentiality statute or regulation.

(2) The term "security incident" means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies. The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected security or privacy incident, or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(3) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(4) With respect to unsecured PHI, the Business Associate is deemed to have discovered a security incident as defined above when the Business Associate either knew, or by exercising reasonable diligence should have been known to an employee of the Business Associate. Upon discovery, the Business Associate must notify VHA of the security incident immediately within one hour of discovery or suspicion as agreed to in the BAA.

(5) 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.

(i) Data breach notification requirements. (1) This contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

(2) The Contractor/subcontractor shall provide notice to VA of a privacy or security incident as set forth in the Security and Privacy Incident Investigation section of this clause. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor 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.

(3) The Contractor/subcontractor shall fully cooperate with VA or any Government agency conducting an analysis regarding any notice of a data breach or potential data breach or security incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for VA, and shall address all relevant information concerning the data breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including—

(A) Date of occurrence;

(B) Date of incident detection;

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of VA control.

(H) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive personal information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(j) Training. (1) All Contractor employees and subcontractor employees requiring access to VA information or VA information systems shall complete the following before being granted access to VA information and its systems:

(i) On an annual basis, successfully complete the VA Privacy and Information Security Awareness and VA Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security

Rules of Behavior for Organizational Users, relating to access to VA information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that VA Information Security Rules of Behavior for Organizational Users signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the VA Information Security Rules of Behavior, within the timeframe required, 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 training and documents are complete.

(k) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and BAAs, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to VA information (including VA sensitive information, i.e., sensitive personal information and protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see VAAR 802.101 definition of information technology-related contracts).

(End of clause)

**VAAR 852.219-73 VA NOTICE OF TOTAL SET-ASIDE FOR CERTIFIED SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESSES (JAN 2023) (DEVIATION)**

(a) *Definition*. For the Department of Veterans Affairs, "*Service-disabled Veteran-owned small business concern or SDVOSB*":

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned 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 or eligible surviving spouses (see VAAR 802.101, Surviving Spouse definition);

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

(iii) The business meets Federal small business size standards for the applicable North American Industry Classification System (NAICS) code identified in the solicitation document;

(iv) The business has been certified for ownership and control pursuant to 38 U.S.C. 8127, 13 CFR 128, and is listed as certified in the SBA certification database at https://veterans.certify.sba.gov/; and

(v) The business agrees to comply with VAAR subpart 819.70 and Small Business Administration (SBA) regulations regarding small business size, government contracting, and the Veteran Small Business Certification Program at 13 CFR parts 121, 125, and 128.

(2) The term "Service-disabled Veteran" 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).

(3) The term "small business concern" has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).

(4) The term "small business concern owned and controlled by Veterans with service-connected disabilities" has the meaning given the term "small business concern owned and controlled by service-disabled veterans" under section 3(q)(2) of the Small Business Act (15 U.S.C. 632(q)(2)).

(5) The term "SDVOSB participant" or certified SDVOSB means a small business that has been certified in the SBA Veteran Small Business Certification Program and listed in the SBA certification database (see 13 CFR 128.102).

(b) *General.* In order for a concern to submit an offer and be eligible for the award of an SDVOSB set-aside or sole source contract, the concern must qualify as a small business concern under the size standard corresponding to the NAICS code assigned to the contract and be listed as an SDVOSB participant in the SBA certification database as set forth in 13 CFR 128.

(1) Offers received from entities that are not certified SDVOSBs and listed in the SBA certification database at the time of offer shall not be considered.

(2) Any award resulting from this solicitation shall be made to a certified SDVOSB listed in the SBA certification database who is eligible at the time of submission of offer(s) and at the time of award.

(3) The requirements in this clause apply to any contract, order or subcontract where the firm receives a benefit or preference from its designation as an SDVOSB, including set-asides, sole source awards, and evaluation preferences.

I *Representation.* Pursuant to 38 U.S.C. 8127(e), only certified SDVOSBs listed in the SBA certification database are considered eligible to receive award of a resulting contract. By submitting an offer, the prospective contractor represents that it is an eligible and certified SDVOSB as defined in this clause, 13 CFR 121, 125, and 128, and VAAR subpart 819.70.

(d) *Agreement/LOS certification.* When awarded a contract action, including orders under multiple-award contracts, an SDVOSB agrees that in the performance of the contract, the SDVOSB shall comply with requirements in VAAR subpart 819.70 and SBA regulations on small business size, and government contracting programs at 13 CFR part 121 and part 125, including the non-manufacturer rule and limitations on subcontracting (LOS) requirements in 13 CFR 121.406(b) and 13 CFR 125.6. For the purpose of limitations on subcontracting, only certified SDVOSBs listed in the SBA certification database (including independent contractors) shall be considered eligible and/or "similarly situated" (i.e., a firm that has the same small business program status as the prime contractor). An otherwise eligible firm further agrees to comply with the

required (LOS) certification requirements in this solicitation (see 852.219-75 or 852.219-76 as applicable). These requirements are summarized as follows:

(1) *Services.* In the case of a contract for services (except construction), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance to firms that are not certified SDVOSBs listed in the SBA certification database (excluding direct costs to the extent they are not the principal purpose of the acquisition and the SDVOSB/VOSB does not provide the service, such as airline travel, cloud computing services, or mass media purchases). When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract.

(2) *Supplies/products.* (i) In the case of a contract for supplies or products (other than from a non-manufacturer of such supplies), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database. When a contract includes both supply and services, the 50 percent limitation shall apply only to the supply portion of the contract.

(ii) In the case of a contract for supplies from a non-manufacturer, the SDVOSB prime contractor will supply the product of a domestic small business manufacturer or processor, unless a waiver as described in 13 CFR 121.406(b)(5) has been granted. Refer to 13 CFR 125.6(a)(2)(ii) for guidance pertaining to multiple item procurements.

(3) *General construction.* In the case of a contract for general construction, the SDVOSB prime contractor will not pay more than 85% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database.

(4) *Special trade construction contractors.* In the case of a contract for special trade contractors, no more than 75% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, may be paid to firms that are not certified SDVOSBs listed in the SBA certification database.

(5) *Subcontracting.* An SDVOSB subcontractor must meet the NAICS size standard assigned by the prime contractor and be certified and listed in the SBA certification database to count as similarly situated. Any work that a first tier VIP-listed SDVOSB subcontractor further subcontracts will count towards the percent of subcontract amount that cannot be exceeded. For supply or construction contracts, the cost of materials is excluded and not considered to be subcontracted. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the portion of the contract with the preponderance of the expenditure upon which the assigned NAICS is based. For information and more specific requirements, refer to 13 CFR 125.6.

(e) Required limitations on subcontracting compliance measurement period. An SDVOSB shall comply with the limitations on subcontracting as follows:

[Contracting Officer check as appropriate.]

__X__ By the end of the base term of the contract or order, and then by the end of each subsequent option period; or

____ By the end of the performance period for each order issued under the contract.

(f) *Joint ventures.* A joint venture may be considered eligible as an SDVOSB if the joint venture 13 CFR 128.402 and the managing joint venture partner makes the representations under paragral(c) of this clause. A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (d) of this clause will be performed by the aggregate of the joint venture participants.

(g) *Precedence.* The VA Veterans First Contracting Program, as defined in VAAR 802.101, subpart 819.70, and this clause, takes precedence over any inconsistencies between the requirements of the SBA Veteran Small Business Certification Program, and the VA Veterans First Contracting Program.

(h) *Misrepresentation.* Pursuant to 38 USC 8127(g), any business concern, including all its principals, that is determined by VA to have willfully and intentionally misrepresented a company's SDVOSB status is subject to debarment from contracting with the Department for a period of not less than five years (see VAAR 809.406-2 Causes for Debarment).

(End of clause)

**VAAR 852.222-71, COMPLIANCE WITH EXECUTIVE ORDER 13899. (DEVIATION) (APR 2025)**

(a)The contractor shall comply with Executive Order 13899, Combating Anti-Semitism, pursuant to Title VI of the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(b)The contractor shall timely disclose, in writing, to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation under Executive Order 13899, Combatting Anti-Semitism pursuant to the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(c)The contractor shall include the terms and conditions of this clause in every subcontract or purchase order so that these terms will be binding on every subcontractor or vendor.

(End of clause)

**VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2018)**

(a) *Definitions.* As used in this clause—

(1) *Contract financing payment* has the meaning given in FAR 32.001;

(2) *Designated agency* office means the office designated by the purchase order, agreement, or contract to first receive and review invoices. This office can be contractually designated as the receiving entity. This office may be different from the office issuing the payment;

(3) *Electronic form* means an automated system transmitting information electronically according to the accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests;

(4) *Invoice payment* has the meaning given in FAR 32.001; and

(5) *Payment request* means any request for contract financing payment or invoice payment submitted by the contractor under this contract.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Data transmission.* A contractor must ensure that the data transmission method and format are through one of the following:

(1) VA's Electronic Invoice Presentment and Payment System at the current website address provided in the contract.

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI).

(d) *Invoice requirements.* Invoices shall comply with FAR 32.905.

(e) *Exceptions*. If, based on one of the circumstances in this paragraph (e), the Contracting Officer directs that payment requests be made by mail, the Contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for—

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of Clause)

**VAAR 852.239-70 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2023)**

(a) *Definitions.* As used in this clause -

*Information technology* has the same meaning in FAR 2.101 and also *means* Information and Communication Technology (ICT).

*Information system security plan* means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

(b) *Responsibilities.* The Contractor shall be responsible for information system security for all systems connected to a Department of Veterans Affairs (VA) network or operated by the Contractor for VA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to VA information that directly supports the mission of VA. Examples of tasks that require security provisions include -

(1) Hosting of VA e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by VA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to VA general support systems/major applications at a level beyond that granted the general public, *e.g.,* bypassing a firewall.

(c) *Information system security plan.* The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. VA information systems must have an information system security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. This plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The information system security plan should include implementation status, responsible entities, resources, and estimated completion dates. Information system security plans may also include, but are not limited to, a compiled list of system characteristics, and key security-related documents such as a risk assessment, PIA, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The plan shall address the specific contract requirements regarding information systems related support or services included in the contract, to include the performance work statement (PWS) or statement of work (SOW). The Contractor's

Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information system security requirements in accordance with Federal and VA policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following.

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines; and

(3) VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(d) *Submittal of plan.* Within 90 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) *Security accreditation.* As required by current VA policy, the Contractor shall submit written proof of information system security accreditation to the Contracting Officer for non-VA owned systems. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with VA policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this accreditation a final information system security plan, such as a risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and the final information system security plan and the accompanying documents, such as a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan.

(f) *Annual validation.* On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the Information System Security Plan remains valid.

(g) *Banners.* The Contractor shall ensure that the official VA banners are displayed on all VA systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system. The Office of Information Technology will make official VA banners available to the Contractor.

(h) *Screening and access.* The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for VA or interconnected to a VA network in accordance with VA Directives and Handbooks referenced in paragraph (c) of this clause.

(i) *Training.* The Contractor shall ensure that its employees performing services under this contract complete VA security awareness training on an annual basis. This includes signing an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723; FAR 39.105, Privacy; clause 852.204-71, Information and Information Systems Security, and this clause on an annual basis.

(j) *Government access.* The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information system inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of VA data or to the function of information systems operated on behalf of VA), and to preserve evidence of computer crime.

(k) *Notification of termination of employees.* The Contractor shall immediately notify the Contracting Officer when an employee who has access to VA information systems or data terminates employment.

(l) *Subcontractor flow down requirement.* The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of Clause)

**VAAR 852.239-71 INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2023)**

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 852.239-70, Security Requirements for Information Technology Resources.

(End of clause)

**VAAR 852.239-72 INFORMATION SYSTEM DESIGN AND DEVELOPMENT (FEB 2023)**

(a) Design or development at non-VA facilities. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with the Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA) regulations,

NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR part 164, subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections (TIC) Reference Architecture).

(b) Privacy Impact Assessment. During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

(c) Security of procured or developed systems and technologies. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that Security Fixes shall not negatively impact the Systems.

(d) Subcontract flow down requirements. The Contractor shall include the clause at 52.224-1, Privacy Act Notification, in every solicitation and/or subcontract awarded by the Contractor when the clause 52.224-1 is included in its contract.

(End of clause)

**VAAR 852.239-73 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE (FEB 2023)**

(a) *Definitions*. As used in this clause—

*Assessment and Authorization (A&A)* means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable VA policies and procedures is the mechanism by which VA provides an Authorization to Operate (ATO), the official management decision given by the VA to authorize operation of an information system (see VA Handbook 6500 for additional details).

*Information system security plan* means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

(b) *Hosting, operation, maintenance, or use at non-VA facilities*. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with the applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) Privacy and Security Rules, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy

handbooks, Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent to or exceed, those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to approval to operate. All external Internet connections to VA's network involving VA information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) *Collecting, processing, transmitting, and storing of VA sensitive information*. Adequate security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the Information System Security Plan and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection, processing, transmitting, and storing of VA sensitive information.

(d) *Annual FISMA security controls assessment*. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the Privacy Impact Assessment. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into VA's POA&M management process. The Contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the VA in the performance work statement (PWS) or statement of work (SOW), or in the approved remediation plan through the VA POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Directive 6500. This may require reviewing and updating all of the documentation as described in VA Handbook 6500.6 (e.g., System Security Plan, Contingency Plan). See VA Handbook 6500.6 for a list of documentation. The VA Information System Risk Management (ISRM) office can provide guidance on whether a new A&A would be necessary.

(e) *Annual self-assessment*. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. VA reserves the right

to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) *Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on VA networks*. VA prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on VA networks. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, PWS, SOW or contract. All of the security controls required for government furnished equipment (GFE) must also be utilized in approved other equipment (OE) at the Contractor's expense. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

(g) *Disposal or return of electronic storage media on non-VA leased or non-VA owned IT equipment*. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with NIST 800-88, Rev. 1, "Guidelines for Media Sanitization," and VA Directive 6500, VA Cybersecurity Program, paragraph 2(b)(5), Media Sanitization including upon—

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (e.g., hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per VA Handbook 6500.10 requirements. This must be completed within 30 days of termination of the contract.

(h) Bio-Medical devices and other equipment or systems. Bio-Medical devices and other equipment or systems containing media (e.g., hard drives, optical disks) with VA sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of VA sensitive information the devices may be provided back to the Contractor under one of three scenarios—

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn-in if VA's initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

**(End of clause)**

**VAAR 852.239-74 SECURITY CONTROLS COMPLIANCE TESTING (FEB 2023)**

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by VA in the event of a security incident or at any other time.

**(End of clause)**

**VAAR 852.239-76 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:

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: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is availa

ble from the Access Board: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule.

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

**Compatibility 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.

**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 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.

(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)**

**VAAR 852.247-71 DELIVERY LOCATION (OCT 2018)**

Shipment of deliverable items, other than reports, shall be sent to: **See Section B.4 Performance Work Statement.**

(End of Clause)

**VAAR 852.247-72 MARKING DELIVERABLES (OCT 2018)**

(a) The contract number shall be placed on or adjacent to all exterior mailing or shipping labels of deliverable items called for by the contract.

(b) Mark deliverables, except reports, for: **See Section B.4 Performance Work Statement.**

**(End of Clause)**

**VAAR 852.247-74 ADVANCE NOTICE OF SHIPMENT (OCT 2018)**

Five workdays prior to shipping item(s). The Contractor shall furnish the anticipated shipment date, bill of lading number (if applicable), and carrier identity to **See Section B.4 Performance Work Statement.**

**(End of clause)**

**(End of Addendum to 52.212-4)**

## SECTION D – ATTACHMENTS AND EXIBITS

## ATTACHMENT A – PRICING EVALUATION SPREADSHEET

## SECTION E - SOLICITATION PROVISIONS*

***This section will be removed from any resultant award.**

### I. RFO 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL ITEMS (DEVIATION DATE: OCTOBER 28, 2025)

### ADDENDUM to RFO 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Provisions that are incorporated by reference (by Citation Number, Title, and Date), have 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 following provisions are incorporated into 52.212-1 as an addendum to this solicitation:

### E.1 INSTRUCTIONS TO OFFERORS - PROPOSAL SUBMISSIONS

1. All proposals will be evaluated by Government personnel in accordance with the written content of the submission. The Government reserves the right to award without discussions. Proposals that fail to meet any material requirement of the solicitation, merely restate the requirement, or state that the requirement will be met without providing supporting rationale, will be rated Not Acceptable and removed from further consideration. Therefore, each initial proposal should contain the Offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct exchanges if later determined by the Contracting Officer to be necessary.

2. The Offeror's proposal shall be submitted electronically by the date and time indicated in the solicitation via juan.perez5@va.gov in the files set forth below. The Offeror's proposal shall consist of four (4) volumes. The Volumes are I -Technical, II – Past Performance, III – Price (Attachment A - Pricing Evaluation Spreadsheet), and IV - Solicitation, Offer and Award Documents. The use of hyperlinks or embedded attachments in proposals is prohibited. Offerors are encouraged to register for the Vendor Portal in order to ensure timely transmission of their proposals to the Government. WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

3. PROPOSAL FILES. Offeror's responses shall be submitted in accordance with the following instructions:

a. Format. The submission shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer. Proposal page limitations are applicable to this procurement. The Table below indicates the maximum page count (when applicable) for each volume of the Offeror's proposal.

All files will be submitted as either a Microsoft Word 2010 (.doc) [if allowing Word documents] Microsoft Excel (.XLS) file or an Acrobat (PDF) file or compatible as indicated in the table. Page size shall be no greater than 8 1/2" x 11" with printing on one side, only. The top, bottom, left and right margins shall be a minimum of one inch (1") each. Font size shall be no smaller than 12-point. Arial or Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos, and headers and footers may be within the page margins ONLY and are not bound by the 12-point font requirement. Footnotes to text shall not be used. All proprietary information shall be clearly and properly marked. If the Offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the Offeror's page limitations unless otherwise indicated in the specific volume instructions below. Pages in violation of these instructions, either by exceeding the margin, font, printing, or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view.

b. File Packaging. All of the proposal files may be compressed (zipped) into one file entitled "proposal.zip" using WinZip version 6.2 or later version or the proposal files may be submitted individually.

c. Content Requirements. All information shall be confined to the appropriate file. The Offeror shall confine submissions to essential matters, sufficient to define the proposal and provide an adequate basis for evaluation. Offerors are responsible for including sufficient details, in a concise manner, to permit a complete and accurate evaluation of each proposal. The titles and page limits requirements for each file are shown in the Table below:

| Volume Number | Factor | File Name | Page Limitations* |
|---|---|---|---|
| Volume I | Technical | Tech.pdf | 10 |
| Volume II | Past Performance | Past Perf.pdf | 6 |
| Volume III | Price | Price.xls | None |
| Volume IV | Solicitation, Offer & Award Documents, Certifications & Representations | OfrRep.pdf | None |

**Page Limitations:** A Cover Page, Table of Contents and/or a glossary of abbreviations or acronyms will not be included in the page count of the Technical Volume. However, be advised that any and all information contained within any Table of Contents and/or glossary of abbreviations or acronyms submitted with an Offeror's proposal will not be evaluated by the Government.

**(i) VOLUME I – TECHNICAL FACTOR.** Offerors shall propose a detailed approach that addresses the elements outlined in the following Specific Tasks and Deliverables of the PWS.

1. **SYSTEM DESIGN, TECHNOLOGY, AND ARCHITECTURE (PWS Sections 3.0, 3.1, 5.1.1, 5.1.2)**
   The Offeror shall describe its technical approach for delivering a unified PEW enterprise architecture aligned with VISN-wide clinical, operational, and technical requirements. The proposal shall detail the methods for conducting workflow discovery, site assessments, system design, coverage modeling, geofencing, capacity planning, data modeling, and accuracy targets. The Offeror shall demonstrate a clear understanding of the VA environment and provide evidence of experience designing RTLS/PEW systems, including integration with nurse call, fire alarm, access control, and other enterprise systems. To receive an acceptable rating, the Offeror must demonstrate the ability to produce all required architecture artifacts and meet the PWS accuracy and interoperability requirements.

2. **TEAMING AND RESELLER REQUIREMENTS (PWS Section 3.2)**
   The Offeror shall identify all Original Equipment Manufacturers (OEMs) associated with the proposed solution and provide documentation demonstrating formal teaming agreements or authorized reseller/distributor status for all proposed hardware, software, and professional services. These agreements must remain in place for the entire Ordering Period. To be rated acceptable or higher, the Offeror must provide clear evidence of valid OEM authorizations for procurement, configuration, installation, integration, and sustainment.

3. **HARDWARE PROVISIONING AND INSTALLATION (PWS Sections 5.1.3, 5.1.6)**
   The Offeror shall describe its approach for providing, staging, and installing hardware components required for PEW prevention systems, including readers,

gateways, exciters, exit controllers, tags, BLE beacons, and other supporting infrastructure. The proposal shall include a complete list of proposed hardware and demonstrate compliance with OEM installation standards. To receive a rating above acceptable, the Offeror shall provide up to three examples of past performance involving installation of PEW/RTLS hardware (e.g., CenTrak, Securitas/WanderGuard, Accutech) in healthcare environments, preferably VA facilities.

4. **SOFTWARE INSTALLATION, CONFIGURATION, AND INTEGRATION (PWS Sections 5.1.7, 5.1.8)**
   The Offeror shall describe its capability to install, configure, and integrate all required software necessary to operate PEW prevention systems, including alerting platforms, device administration tools, data synchronization components, and enterprise system connectors. The proposal shall demonstrate understanding of required cybersecurity configurations, interface integrations (e.g., nurse call, access control), and VA system baselines. To obtain a rating above acceptable, the Offeror must provide evidence of experience performing system administration, software configuration, and enterprise-system integration in clinical environments, including VA or similar healthcare networks.

5. **WARRANTY, OPERATIONS, AND SUSTAINMENT SERVICES (PWS Section 5.2.3 and Section 3.0 – Operations & Sustainment)**
   The Offeror shall describe its capability to provide warranty services, operations support, and long-term sustainment of PEW systems in accordance with the PWS. This includes preventive and corrective maintenance, tiered support, system monitoring, optimization reviews, and help desk responsiveness. To achieve a rating higher than acceptable, the Offeror shall describe its sustainment methodology and provide up to three past performance examples involving ongoing maintenance and support of PEW, RTLS, or similar patient safety systems in healthcare facilities.

**(ii) VOLUME II – PAST PERFORMANCE FACTOR.** Offerors shall submit up to three contracts (including Federal, State, local government, or private) (prime contracts, task/delivery orders, and/or major subcontracts defined as performing 20% or more effort) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation. Areas of relevance include delivery of hardware and software and installation and maintenance of real-time location solutions in a clinical environment. Data concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order. This volume shall be organized into the following sections:

(1) Section 1 – Contract Descriptions. This section shall include the following information:

(a) Contractor/Subcontractor place of performance, CAGE Code and DUNS Number. If the work was performed as a subcontractor, also provide the name of the prime contractor and Point of Contact (POC) within the prime contractor organization (name, and current address, e-mail address, and telephone number).

(b) Contracting activity, and current address, Procuring Contracting Officer's name, e-mail address, and telephone number.

(c) Technical representative/Contracting Officer's Representative (COR), and current e-mail address, and telephone number.

(d) Contract administration activity and the Administrative Contracting Officer's name, and current e-mail address, and telephone number.

(e) Contract Number and, in the case of Indefinite Delivery type contracts, GSA contracts, and Blanket Purchase Agreements, including Delivery Order Numbers.

(f) Contract Type (specific type such as Fixed Price (FP), Cost Reimbursement (CR), Time & Materials (T&M), etc.) In the case of Indefinite Delivery contracts, indicate specific type (Requirements, Definite Quantity, and Indefinite Quantity) and secondary contract type (FP, CR, T&M, etc).

(g) Awarded price/cost.

(h) Final or projected final price/cost.

(i) Original delivery schedule, including dates of start and completion of work.

(j) Final or projected final, delivery schedule, including dates of start and completion of work.

(2) Section 2 - Performance. Offerors shall provide a specific narrative explanation of each contract listed in Section 1 describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation. For any contract(s)/task order(s) that did not/do not meet original schedule or technical performance requirements, provide a brief explanation of the reason(s) for the shortcoming(s) and any corrective action(s) taken to avoid recurrence. The Offerors shall list each time the delivery schedule was revised and provide an explanation of why the revision was necessary. The Offerors shall indicate if any of the contracts listed were terminated and the type and reasons for the termination.

(3) Section 3 – Subcontracts. Offerors shall provide an outline of how the effort required by the solicitation will be assigned for performance within the Offeror's corporate entity and among the proposed subcontractors. The information provided for the prime Offeror and each proposed major subcontractor must include the entire company name,

company address, CAGE Code, DUNS Number and type of work to be performed by citing the applicable Government PWS paragraph number.

(4) Section 4 – New Corporate Entities. New corporate entities may submit data on prior contracts involving its officers and employees. However, in addition to the other requirements in this section, the Offeror shall discuss in detail the role performed by such persons in the prior contracts cited. Information should be included in the files described in the sections above.

**(iii) VOLUME III– PRICE.** The Offeror shall complete Attachment A. Offerors are advised that the quantities identified in Attachment A are for evaluation purposes only. Offerors shall not adjust quantities. Offerors shall insert a unit price in each ordering period and ensure the total price for each line item calculates correctly with no rounding issues.

Price Rounding Issue - Offerors are advised that the quantities identified in Attachment A are for evaluation purposes only. Offerors shall not adjust quantities. Offerors shall insert a unit price in each ordering period and ensure the total price for each line item calculates correctly with no rounding issues.

Offerors should propose using an estimated award date of August 2026.

**(iv) VOLUME IV - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS.**

Certifications and Representations - An authorized official of the firm shall sign the SF 1449 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

a. Solicitation Section A – Standard Form SF1449 and Acknowledgement of Amendments, if any.
b. Appropriate response to VAAR clause(s) found in section C.
c. Any proposed terms and conditions and/or assumptions upon which the proposal is predicated.

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 proposal Unacceptable, and thus ineligible for award. Please be guided in your submission, accordingly. In accordance with RFO 12.107(b), the Government will not accept any terms and conditions that are contained within hyperlinks or that reference hyperlinks. All proposed terms and conditions must be included in full within the submitted quotation. Hyperlinked T&Cs, or documents containing T&Cs accessed via hyperlink, will not be reviewed or incorporated.

(End of Provision)

**E.2 RFO 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/far-overhaul/far-part-deviation-guide/far-overhaul-part-52#FAR_52_252_2 (RFO)

http://www.va.gov/oal/library/vaar/index.asp (VAAR)

(End of Provision)

| RFO Number | Title | Date |
|---|---|---|
| 52.203-18 | PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS-REPRESENTATION | JAN 2017 |
| 52.204-7 | SYSTEM FOR AWARD MANAGEMENT | DEVIATION OCT 2025 |
| 52.204-16 | COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING | AUG 2020 |
| 52.209-2 | PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS-REPRESENTATION | DEVIATION OCT 2025 |
| 52.212-1 | INSTRUCTIONS TO OFFERORS-COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES | DEVIATION OCT 2025 |
| 52.217-5 | EVALUATION OF OPTIONS | DEVIATION OCT 2025 |
| 52.229-11 | TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION | JUN2020 |
| 52.240-90 | SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS | DEVIATION OCT 2025 |

**E.3 RFO 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (DEVIATION OCT 2025)**

(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.4 RFO 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (DEVIATION OCT 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 paragraph (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 occurrence 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 paragraph (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.5 RFO 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (DEVIATION OCT 2025)**

(a) 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.6 RFO 52.216-1 TYPE OF CONTRACT (DEVIATION OCT 2025)**

The Government contemplates award of a Firm-Fixed-Price, indefinite-delivery, indefinite-quantity contract resulting from this solicitation.

**(End of Provision)**

## E.7 RFO 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Hand-Carried Address:
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

Mailing Address:

Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

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

(End of Provision)

**E.8 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (SEP 2018)**

(a) Any protest filed by an interested party shall—

(1) Include the name, address, fax number, email and telephone number of the protester;

(2) Identify the solicitation and/or contract number;

(3) Include an original signed by the protester or the protester's representative and at least one copy;

(4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;

(5) Specifically request a ruling of the individual upon whom the protest is served;

(6) State the form of relief requested; and

(7) Provide all information establishing the timeliness of the protest.

(b) Failure to comply with the above may result in dismissal of the protest without further consideration.

(c) Bidders/offerors and Contracting Officers are encouraged to use alternative dispute resolution (ADR) procedures to resolve protests at any stage in the protest process. If ADR is used, the Department of Veterans Affairs will not furnish any documentation in an ADR proceeding beyond what is allowed by the Federal Acquisition Regulation.

(End of Provision)

**E.9 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (SEP 2018)**

(a) As an alternative to filing a protest with the Contracting Officer, an interested party may file a protest by mail or electronically with: Executive Director, Office of Acquisition and Logistics, Risk Management and Compliance Service (003A2C), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or Email: *EDProtests@va.gov.*

(b) The protest will not be considered if the interested party has a protest on the same or similar issue(s) pending with the Contracting Officer.

(End of Provision)

## E.10 VAAR 852.239-75 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2023)

(a) Any offeror responding to this solicitation must comply with established VA Information and Communication Technology (ICT) (formerly Electronic and Information (EIT)) accessibility standards. Information about Section 508 is available at http://www.section508.va.gov/.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 852.239-75, Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit appropriate VA Section 508 Checklists, in accordance with the checklist completion instructions. The purpose of the checklists is to assist VA acquisition and program officials in determining whether proposed ICT supplies, or information, documentation and services conform to applicable Section 508 accessibility standards. The checklists allow offerors or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues.

(c) Respondents to this solicitation must identify any exception to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(End of provision)

## II. RFO 52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION OCT 2025)

## A. BASIS FOR AWARD

The Government intends to make a single award to the offeror whose proposal represents the best value to the Government in accordance with a best value trade-off source selection. Award may be made to other than the lowest-priced offeror or the highest technically rated offeror when the Contracting Officer determines that a higher-priced or lower-priced offer provides a more advantageous solution to the Government.

The following evaluation factors shall be used to determine best value:

• Factor I – Technical

• Factor II – Past Performance
• Factor III – Price

The Technical Factor is significantly more important than Past Performance, and Past Performance is slightly more important than Price. When combined, the non-Price Factors are significantly more important than the Price Factor.

To be eligible for award, an offeror must receive a rating of Acceptable or higher under the Technical Factor. Offerors are cautioned that an award may not necessarily be made to the lowest-priced offeror.

## B. FACTORS TO BE EVALUATED

**FACTOR I Volume I** – Technical
**FACTOR II Volume II** - Past Performance
**FACTOR III Volume III** - Price

## C. EVALUATION APPROACH

All proposals will be evaluated by Government personnel in accordance with the written content of the submission. The Government reserves the right to award without discussions. Proposals that fail to meet any material requirement of the solicitation, merely restate the requirement, or state that the requirement will be met without providing supporting rationale, will be rated Not Acceptable and removed from further consideration. Therefore, each initial proposal should contain the Offeror's best terms from a cost or price and technical standpoint. However, the Government reserves the right to conduct exchanges if later determined by the Contracting Officer to be necessary

### 1. TECHNICAL EVALUATION APPROACH:

The Government will evaluate the degree to which the offeror's proposal demonstrates:

**i. Understanding of the Requirement -**
The extent to which the proposal demonstrates a clear, comprehensive understanding of the scope, challenges, and performance requirements and identifies any significant uncertainties with reasonable resolutions.

**ii. Feasibility and Effectiveness of the Approach -**
The extent to which the proposed technical approach is workable, achievable, and provides the Government confidence that requirements will be met or exceeded in a timely and efficient manner.

### 2. PAST PERFORMANCE EVALUATION APPROACH.

Past performance will be assessed to determine the Government's level of confidence in the offeror's ability to perform the required effort successfully. The Government will evaluate up to three contracts (including Federal, State, local government, or private) (prime contracts, task/delivery orders, and/or major subcontracts defined as performing 20% or more effort) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation. Areas of relevance include delivery of hardware and software and installation and maintenance of real-time location solutions. Data concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order.

The Government may use information provided by the offeror, obtained from CPARS, or obtained from any other reliable sources.

Offerors with no relevant past performance history will receive a "Neutral" assessment and will not be evaluated favorably or unfavorably.

**3. PRICE EVALUATION APPROACH.**

For this fixed-price requirement, the Government will evaluate price by multiplying the offeror's proposed unit prices by the Government's estimated quantities for each line item and summing all extended totals. Price will be evaluated for reasonableness and completeness. All calculations will be performed using the offeror's completed "Attachment A – Pricing Evaluation Spreadsheet." Note that estimated quantities will be removed from the attachment before incorporating into the final contract award.

(End of Provision)

**(End of Addendum to 52.212-2)**