

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the SAM database. Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via SAM accessed through <https://www.acquisition.gov>.

(u) *Unauthorized Obligations.*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government 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:

(i) Any such clause is unenforceable against the Government.

(ii) 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 EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or 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.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference.* The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of Clause)

ADDENDUM to FAR 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS

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

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

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

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm>

<u>FAR Number</u>	<u>Title</u>	<u>Date</u>
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION)	FEB 2015
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	MAY 2011
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE	JUL 2016
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	OCT 2014
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-14	RIGHTS IN DATA—GENERAL	MAY 2014
52.227-17	RIGHTS IN DATA—SPECIAL WORKS	DEC 2007
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	DEC 2013

(End of Clause)

C.3 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

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

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements and procedures.* (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of Clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 24 months.

(End of Clause)

C.5 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising

in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.6 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

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

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

(2) *Designated agency office* has the meaning given in 5 CFR 1315.2(m).

(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.

(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. (See Web site at <http://www.fsc.va.gov/einvoice.asp>.)

(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). The X12 EDI Web site (<http://www.x12.org>) includes additional information on EDI 810 and 811 formats.

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

(e) *Exceptions.* If, based on one of the circumstances below, 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)

C.7 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of the state in which the majority of the work will take place. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.8 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

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 shall be furnished to the contractor.

(End of Clause)

C.9 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(3) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(4) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

(4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (OCT 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

(6) 52.204-14, Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

(7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

(8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (OCT 2015) (31 U.S.C. 6101 note).

(9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

(10) [Reserved]

(11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

(ii) Alternate I (NOV 2011) of 52.219-3.

(12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

(ii) Alternate I (JAN 2011) of 52.219-4.

(13) [Reserved]

(14)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

(ii) Alternate I (NOV 2011).

(iii) Alternate II (NOV 2011).

(15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

(ii) Alternate I (Oct 1995) of 52.219-7.

(iii) Alternate II (Mar 2004) of 52.219-7.

(16) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)).

(17)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2017) (15 U.S.C. 637(d)(4)).

(ii) Alternate I (NOV 2016) of 52.219-9.

(iii) Alternate II (NOV 2016) of 52.219-9.

(iv) Alternate III (NOV 2016) of 52.219-9.

(v) Alternate IV (NOV 2016) of 52.219-9.

(18) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

(19) 52.219-14, Limitations on Subcontracting (JAN 2017) (15 U.S.C. 637(a)(14)).

(20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

(22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).

(23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (DEC 2015) (15 U.S.C. 637(m)).

(24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015) (15 U.S.C. 637(m)).

(25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

(26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (JAN 2018) (E.O. 13126).

(27) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(28) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(29) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(30) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(31) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

(32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

(33)(i) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(ii) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(34) 52.222-54, Employment Eligibility Verification (OCT 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

(35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

(ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

(36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).

(37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).

(38)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).

(ii) Alternate I (OCT 2015) of 52.223-13.

(39)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).

(ii) Alternate I (JUN 2014) of 52.223-14.

(40) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

(41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).

(ii) Alternate I (JUN 2014) of 52.223-16.

(42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)

(43) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).

(44) 52.223-21, Foams (JUN 2016) (E.O. 13693).

(45) (i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(ii) Alternate I (JAN 2017) of 52.224-3.

(46) 52.225-1, Buy American—Supplies (MAY 2014) (41 U.S.C. chapter 83).

(47)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

(ii) Alternate I (MAY 2014) of 52.225-3.

(iii) Alternate II (MAY 2014) of 52.225-3.

(iv) Alternate III (MAY 2014) of 52.225-3.

(48) 52.225–5, Trade Agreements (OCT 2016) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

(49) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

(50) 52.225–26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

(52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

(53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

(54) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

(55) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013) (31 U.S.C. 3332).

(56) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

(57) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

(58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

(59) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(12)).

(60)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

(ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495).

(2) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(3) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[] (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

[] (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

[] (8) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

[] (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

[] (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792).

[] (11) 52.237-11, Accepting and Dispensing of \$1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities.

(iv) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(v) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(vi) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(vii) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(viii) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(ix) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

(x) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(xii)(A) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xv) 52.222-54, Employment Eligibility Verification (OCT 2015) (E. O. 12989).

(xvi) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

(xvii) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xviii)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(B) Alternate I (JAN 2017) of 52.224-3.

(xix) 52.225–26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xx) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

D.1 - Business Associate Agreement.

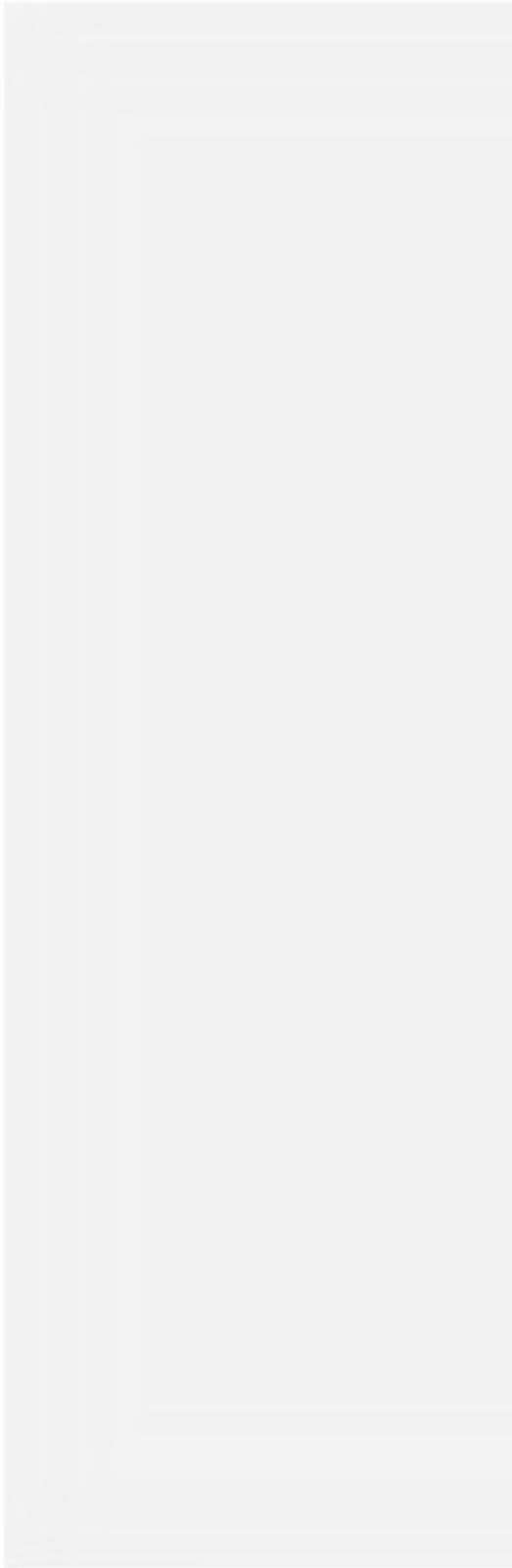


Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS3

- B.1 GOVERNING LAW3
- B.2 CONTRACT ADMINISTRATION DATA4
- B.3 PRICE SCHEDULE5
- B.4 PERFORMANCE WORK STATEMENT 11

SECTION C - CONTRACT CLAUSES52

- C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (JAN 2017)52
- C.2 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998).....59
- C.3 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)60
- C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) ...62
- C.5 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)62
- C.6 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)62
- C.7 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)64
- C.8 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)64
- C.9 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)64

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS\.....73

- D.1 Business Associate Agreement.....54

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations ("FAR"), shall govern this Order. Commercial license agreements may be made a part of this Order but only if both parties expressly make them an addendum. 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 Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap) or 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 Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this 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 Order. Federal law and regulation, including without limitation, the Contract Disputes Act (41 U.S.C. §601-613), the Anti-Deficiency Act (31 U.S.C. §1341 et seq.), the Competition in Contracting Act (41 U.S.C. §253), the Prompt Payment Act (31 U.S.C. §3901, et seq.) and FAR clauses 52.212-4, 52.227-14, 52.227-19 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 Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 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 Order must be made by order modification (Standard Form 30). Nothing in this Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.2 CONTRACT ADMINISTRATION DATA

(continuation from Standard Form 1449, block 18A.)

1. CONTRACT ADMINISTRATION: All contract administration matters will be handled by the following individuals:

a. CONTRACTOR: Televeda
1 North 1st St. Suite #603
Phoenix, AZ 85004
CAGE:
UEI:

Technical POC
(b)(6)
1 North 1st St. Suite #603
Phoenix, AZ 85004
520-955-(b)(6)
(b)(6)@televeda.com

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

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

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: upon receipt of deliverables

- a. Quarterly
- b. Semi-Annually
- c. Other Upon acceptance of deliverables in accordance with B.3
Price Schedule

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.

B.3 PRICE SCHEDULE (this will be completed AFTER Section 5 is completed)

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

BASE PERIOD					
LINE ITEM	DELIVERABLE	QTY	UNIT	UNIT PRICE	TOTAL
	<p>Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs.</p> <p>This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, project management, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs.</p> <p>Period of Performance (PoP) shall be September 30, 2018 – September 29, 2019.</p> <p>Electronic submission to: VA Program Manager (PM), Contracting Officer Representative (COR) and Contracting Officer (CO).</p>				
0001	<p>Inspection: destination Acceptance: destination</p>	12	MO	Not Separately Priced (NSP)	NSP
0001AA	<p>Project Kickoff Meeting Agenda IAW PWS Paragraph 5.1.1</p> <p>Due: Five days prior to the Technical Kickoff Meeting.</p>	1	EA	NSP	NSP
0001AB	<p>Project Kickoff Meeting Minutes IAW PWS Paragraph 5.1.1</p>	1	EA	NSP	NSP

	Due: Three days after the Technical Kickoff Meeting				
0001AC	Contractor Project Management Plan IAW PWS Paragraph 5.1.2 Due 30 days after contract (DAC) award and updated monthly thereafter	1	LO	NSP	NSP
001AD	Monthly Progress Report IAW PWS Paragraph 5.1.3 Due on the fifth day of each month throughout the PoP.	1	LO	NSP	NSP
0001AE	Teleconference Progress Meeting Minutes IAW PWS Paragraph 5.1.3 Due two days after the Teleconference Progress Meetings	1	LO	NSP	NSP
0001AF	Collaboration Agreements from VA/and VSO PWS Paragraph 5.1.4 Due 30 DAC award	1	EA	NSP	NSP
0001AG	Paragraph 5.1.4 Due 30 DAC award	1	EA	NSP	NSP
0001AH	Contractor Staff Roster IAW PWS Paragraph 6.2.2 Due 3 DAC award and updated within one day of any changes in employee status.	1	EA	NSP	NSP
0002	Initial Phase shall be provided IAW PWS Paragraph 5.2, and all of its subparagraphs. This FFP CLIN includes all labor, materials, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.2, inclusive of all subparagraphs. Period of Performance (PoP)	1	LO	NSP	NSP

	shall be September 30, 2018 – September 29, 2019. Electronic submission to: VA PM, COR and CO. Inspection: destination Acceptance: destination				
0002AA	IAW PWS paragraph 5.2.2 Due 30 after	1	EA		
0002AB	IAW PWS paragraph 5.2.2 Due 30 days after completion of Interviews	1	EA		
0002AC	Usability Testing Results IAW PWS paragraph 5.2.2 Due 30 days after completion of Usability Testing	1	EA		
0002AD	IAW PWS paragraph 5.2.2 Due 30 days after completion of Interviews	1	EA		
0002AE	IAW PWS paragraph 5.2.1 Due 120 DAC award	1	EA		
0002AF	IAW PWS paragraph 5.2.1 Due 120 DAC award	1	EA		
0002AG	Year 1 Final Report IAW PWS paragraph 5.2.3 Due 360 DAC award	1	EA		
TOTAL BASE PERIOD					
OPTION PERIOD ONE					
This Option may be exercised in accordance with FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer					
LINE ITEM	DELIVERABLE	QTY	UNIT	UNIT PRICE	TOTAL
1001	Project Management shall be provided IAW PWS Paragraph 5.1, and all of its subparagraphs, except 5.1.1. This FFP CLIN includes all labor, materials, and	12	MO	Not Separately Priced (NSP)	NSP

	<p>deliverables required for the successful completion of the services detailed in PWS Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs..</p> <p>The PoP shall be 12-months commencing immediately upon expiration of the Base Period.</p> <p>Electronic submission to: VA Program Manager (PM), Contracting Officer Representative (COR) and Contracting Officer (CO).</p> <p>Inspection: destination Acceptance: destination</p> <p>The cost of CLIN 1001 shall be included in and allocated to CLINs 1002.</p>				
1001AA	<p>Contractor Project Management Plan IAW PWS Paragraph 5.1.2</p> <p>Due 30 days after commencement of Option and updated monthly thereafter</p>	1	LO	NSP	NSP
1001AB	<p>Monthly Progress Report IAW PWS Paragraph 5.1.3</p> <p>Due on the fifth day of each month throughout the PoP.</p>	1	LO	NSP	NSP
1001AC	<p>Teleconference Progress Meeting Minutes IAW PWS Paragraph 5.1.3</p> <p>Due two days after the Teleconference Progress Meetings</p>	1	LO	NSP	NSP
1001AD	<p>IAW PWS Paragraph 5.1.4</p> <p>Due 30 days after commencement of Option</p>	1	EA	NSP	NSP
1001AE	<p>IAW PWS Paragraph 5.1.4</p>	1	EA	NSP	NSP

	Due 30 days after commencement of Option Contractor Staff Roster IAW PWS Paragraph 6.2.2				
0001AF	Due within one day of any changes in employee status.	1	EA	NSP	NSP
1002	<p>Pilot Study shall be provided IAW PWS Paragraph 5.3, and all of its subparagraphs.</p> <p>This FFP CLIN includes all labor, materials, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.3, inclusive of all subparagraphs.</p> <p>The PoP shall be 12-months commencing immediately upon expiration of the Base Period</p> <p>Electronic submission to: VA PM, COR and CO.</p> <p>Inspection: destination Acceptance: destination</p>	1	LO	NSP	NSP
1002AA	Site-Specific Pilot Study Implementation Plans IAW PWS paragraph 5.3.1.1 Due 90 days after commencement of Option Period	1	EA		
1002AB	IAW PWS paragraph 5.3.1.2 Due 240 days after commencement of Option	1	EA		
1002AC	IAW PWS paragraph 5.3.1.2 Due 240 days after commencement of Option	1	EA		
1002AD	Year 2 Final Report IAW PWS paragraph 5.3.1.3 Due 360 days after commencement of Option	1	EA		

TOTAL BASE PERIOD	
TOTAL AMOUNT (BASE + OPTION PERIOD)	

B.4 PERFORMANCE WORK STATEMENT



**PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Veteran's Health Administration (VHA)
VHA Innovation Ecosystem (14HIL1)**

Talking Circles for Native Veterans

**Date: 10 February 2025
PWS Version Number: 1.5**

1.0 BACKGROUND

As an innovation engine within the Department of Veterans Affairs, the vision of the Veterans Health Administration's Innovation Ecosystem (VHAIE) is a VA continuously innovating at the forefront of science and research, service delivery and implementation of solutions, and employee empowerment. VHAIE leads this vision by fostering organizational capability, delivering operational and clinical breakthroughs, and driving futures. VHAIE is committed to developing and employing agile mechanisms that allow VA to source incremental and transformational innovations to best serve Veterans and their families.

This Broad Agency Announcement (BAA) opportunity seeks to source and fund early-stage research, development, prototyping, field testing, and implementation piloting with an overall goal of moving forward the state of the art.

Through this BAA, VHAIE invites all potential offerors (including private sector companies, non-profits, and institutions of higher learning) to contribute ideas for innovations in SUICIDE prevention, care coordination, and treatment that significantly increase Veteran access to services, reduce or control costs of delivering those services, enhance the performance of VA operations, and improve the quality of service that Veterans and their families receive.

The significant and unprecedented challenges this country faced in 2021 fuel the continued call to action related to a whole-of-government and whole-of-nation approach to suicide prevention. Suicide is a complex problem requiring a full public health approach involving community prevention and clinical intervention. VA services are a critical part of this public health approach.

The data spanning 20 years reveals that Veterans engaged in VHA care have shown a less sharp rise in suicide rates, underscoring the importance of VHA care. Over 20 years of Veteran suicide data also reveal a substantial reduction in suicide rates, specifically for Recent Veteran VHA Users with mental health or substance use disorder diagnoses (77.8 per 100,000 in 2001 to 58.2 per 100,000 in 2021), falling 32.9% for Veterans with depression, 27.6% for those with posttraumatic stress disorder, 26.9% for those with anxiety and 40.4% for those with sedative use disorder. Comparing Veterans with Recent VHA use to other Veterans, we also find notable trends. While overall rates of Veteran suicide rose across the 20 years, age-adjusted suicide rates rose 24.5% for male Veterans with Recent VHA use compared to 62.6% for male Veterans without Recent VHA use. While less notable for women Veterans, the age-adjusted suicide rates rose 87.1% for female Veterans with Recent VHA use and 93.7% for female Veterans without Recent VHA use. Likewise, when looking more specifically across 2020 and 2021, we find the greatest increase in unadjusted rates for Veterans who were neither engaged with VHA nor with VBA. From 2020 to 2021, there were also notable decreases for particular subpopulations of Veterans with Recent VHA use, including those between ages 55- and 74-years-old (overall suicide rate -2.2%, -0.6% for men, -24.9% for women), males between ages 18- and

34-years-old (overall suicide rate -1.9%) and males aged 75-years-old and older (overall suicide rate -8.6%). These findings underscore the importance of continuing to expand access to and engagement of Veterans in VHA and VBA services, as over 50% of Veterans who died by suicide in 2021 had not been engaged in either service. Yet, in order to address the complex interweaving of individual, relational, community and societal risks, VA must continue to fully engage with other federal agencies; public-private partnerships; government at the local, state and 32 As noted above, Veterans receiving VHA care show evidence of higher risk with being more likely to have lower annual incomes, poorer self-reported health status, more chronic medical conditions, and self-reported disability due to physical or mental health factors, greater depression and anxiety, and greater reporting of trauma, lifetime psychopathology, and current suicidality. 10 national levels; VSOs; and local communities to reach all Veterans to support the implementation of a full public health approach, as outlined in the White House Strategy Reducing Military and Veteran Suicide (2021) 33 and VA's National Strategy for Preventing Veteran Suicide (2018). 34 These guiding documents have been operationalized through SP 2.0; Suicide Prevention Now initiative (SP Now); new laws, including the 2020 Commander John Scott Hannon Veterans Mental Health Care Improvement Act; the Veterans Comprehensive Prevention, Access to Care and Treatment Act (COMPACT) of 2020; the National Suicide Hotline Designation Act of 2020; and emerging innovations combined with research and program evaluation. As 2021 has again shown, this public health approach must include both community-based prevention and clinical interventions to reduce suicide in the Veteran population. As we reflect on the core of what we learned about Veteran suicide in 2021, 7 themes emerge for our call to action (see summary listing and description below). While no one solution can address the complexity of all factors involved in suicide, the data clearly outlines that significant reductions in Veteran suicide will not occur without meaningful focused effort to address Veteran firearm suicide. While we vigorously pursue enhanced policies, research, and programs to effectively address the broader socioecological and individual risk and protective factors which speak to "why" a Veteran may consider suicide, we must address directly the "how" of Veteran suicide. It is inescapable that the "how" in 72% of Veteran suicide deaths is firearm compared to 52% of non-Veteran U.S. adult suicides.

VHAIE, therefore, begins our call to action with a focus on primary topic areas that take into account the many facets of suicide prevention, including topics like the "how" of suicide, the importance of a community-led approach to preventing suicide, improved training, or increased access to care. To address the need for innovation in Suicide Prevention, VA seeks innovations across 7 primary topic areas:

- Promote firearm secure storage for Veteran suicide prevention.
- Implement and sustain community collaborations focused upon community-specific Veteran suicide prevention plans.
- Continue expansion of readily accessible crisis intervention services.

- Improve tailoring of prevention and intervention services to the needs, issues, and resources unique to Veteran subpopulations.
- Advance suicide prevention meaningfully into non-clinical support and intervention services, including financial, occupational, legal, and social domains.
- Increase access to and utilization of mental health across a full continuum of care.
- Integrate suicide prevention within medical settings to reach all Veterans.

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 Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules"
2. 10 U.S.C. § 2224, "Defense Information Assurance Program"
3. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
8. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
16. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
17. VA Handbook 6500.6, "Contract Security," March 12, 2010
18. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
19. OI&T Process Asset Library (PAL), <https://www.va.gov/process/>. Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp> NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
20. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015

21. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
22. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
23. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
24. 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
25. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
26. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
27. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
28. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
29. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
30. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
31. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
32. 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>)
33. 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>))
34. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
35. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
36. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
37. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
38. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
39. [The Veteran Metrics Initiative Well-Being Inventory, https://www.ptsd.va.gov/professional/assessment/documents/WellBeingAssessment.pdf](https://www.ptsd.va.gov/professional/assessment/documents/WellBeingAssessment.pdf)

3.0 SCOPE OF WORK

This contract and proposed solution focus on the following topic:

- Improve tailoring of prevention and intervention services to the needs, issues, and resources unique to Veteran subpopulations.

Topic Detail: Creating tailored and responsive interventions to meet each population's needs will be required to address what 2021 revealed to us, with growing rates in American Indian/ Alaska Native Veteran populations (AIANV), younger Veterans, transitioning Service member populations, women Veterans and more, as seen in the data for 2021. A one-size-fits-all Veteran suicide prevention strategy will not be effective in meeting the needs of the diverse population of Veterans.

3.1 Specific Problem to Address with this Solution:

There is an unmet medical, ethical, and moral need for tailored approaches to peer support that integrate community competence, address specific social and economic contexts, and leverage community resources to improve social connections and overall health. This solution will address engagement and culturally competent resources for AIAN Veterans and women Veterans.

3.1.1 Background of Problem:

According to the VA, there are currently more than 140,000 AIANV (self-identified). Director Baldwin of the Navajo Nation VA (NNVA) reported there are upwards of 30,000 Navajo military veterans 15,000 to 20,000 of whom reside on the reservation and about 2,800 of whom are women Veterans. Given that AIANV have the highest suicide rates amongst all demographics (51.8% increase), targeted interventions here would really move the needle. Primary focus remains on prioritizing Indigenous Veterans, but this neatly intersects with Women and Rural veteran subpopulations. There are 650,000 women veterans, and they experience 166% higher suicide rates than non-Veteran women. According to VA ORH, a quarter of all veterans (4.4 Million) live in rural areas, and have higher rates of suicide and trouble accessing care than their urban counterparts. These subpopulations have unique experiences that increase the risk of suicide (historical trauma, military sexual trauma, substance abuse, etc.) and require targeted resources & solutions.

3.2 Proposed Solution:

In 2023, the VA's Mission Daybreak launched Televeda's "Hero's Story Project" (HSP). The HSP is a comprehensive suicide prevention program tailored for Native American veterans incorporating traditional healing practices, such as talking circles and storytelling, in an evidence-based Peer Support (PS) modality. The HSP innovation comprises (a) "Virtual Talking Circles" (VTC) web application and (b) "HSP Storytelling Curriculum", a narrative therapy PS framework. Overall, the HSP is a novel re-imagining of peer support in a culturally competent way to aid with building trust and, ultimately, the project aims to foster peer collaboration that improves social connectedness and resource navigation via engaged journeys. Televeda shall use the Hero's Story model to

expand culturally relevant peer support (Virtual Talking Circles) by targeting minority Veteran sub-populations with personalized resource journeys, prioritizing AI/AN (with Women/MST and rural intersection). HSP Sessions can be hosted in person, virtually or hybrid. The data corroborates that Veterans are also more likely to first engage with peer or support groups before a therapist. Once they're comfortable in a peer setting Veterans may express vulnerable social needs and Televeda will then leverage the BRAVE Journeys with peer support interactions to build a trusting environment to connect participants with needed resources. **This proposed work will focus on the expansion of the HSP solution to additional partners and locations as well as a more robust evaluation of HSP, including associated Virtual Talking Circles and low-tech connection to resources.**

Honoring Native traditions, Televeda proposes to design "resource journeys" that build direct ties between AIANV and the VA that helps engagement, trust-building and connecting veterans to protective resources. This storytelling-approach fosters individual motivation ("call to adventure" via our resource modules) and a sense of purpose for the Veterans, while also contributing back to the community supporting their family/tribe by bringing back wisdom to the people (knowledge-sharing/resource ratings). Such journeys would contribute to the transmission of important cultural knowledge and experiences that are beneficial for both the community and the VA.

While each veteran subpopulation is unique, key issues – Trust, Access, Isolation – are exacerbated for AIANV. American Indian & Alaskan Native Veterans (AIANV) rarely engage with the VA because of historical mistrust, access to care is fraught by transportation & physical challenges with no culturally appropriate resources, and social isolation is lethal on the reservation. The HSP builds pathways to trust, increases access to care, and facilitates the delivery of traditional healing through a culturally competent and accessible interface. Suicide prevention is addressed in an upstream approach by fostering resilience, social connectedness and community healing. The platform is designed to lower social isolation and promote overall well-being by facilitating meaningful connections. Televeda aims to address the complex contributing factors to suicide for AIANV by matching them with essential health-related social needs (protective factors), reducing the risk of suicidal ideation.

Medical mistrust leads to lower engagement with healthcare systems. Through the BRAVE Journey, the goal is to build trust and help connect previously unconnected AIANV and women Veterans with the VA. Commendably, VA trust scores are the highest in its history. Unfortunately, that success has not translated over to AIANV (lowest scoring at 69.9%). That is significantly lower than all the other groups. The trust experience of Women Veterans was slightly lower than that of males, but in cases of MST survivors, the risk of being triggered in these settings was much higher. For instance, multiple attendees of women's virtual talking circles commented that they preferred to speak with peers outside of the VA setting and that they felt safe to discuss sensitive issues because they were within their homes and able to speak after putting their kids to bed. During Co-design interviews, one Native leader remarked: "What is the point of increasing engagement for AIANV to visit the VA when they will have poor experiences?" Another concern VA clinical professionals flagged was related to the initial concept proposal of AI-based peer matching to group cohorts by "lived experience". It was noted that in clinical group therapy sessions having diverse members helps with the healing process.

This project fulfills the objective of developing a targeted solution for veteran subpopulations. There is a need for a tailored lens to focus on the top priority specialty population, American Indian (AI) and American Native (AN), which have the highest rate of suicide, and that intersects with women Veterans (overwhelming feedback and community respect for women-only sessions) which is the fastest growing demographic afflicted by suicide. This project increases understanding of Veteran subpopulations and develops a unique service delivery model for specialty populations.

Phase 1 and Phase 2 will include development of formal partnerships with additional VSOs and tribal organizations via Memorandums of Understanding (MOUs) between Contractor and those partners.

Testing will occur, across both phases, in two states, Arizona and New Mexico. Initiation of Phase 2 is dependent on satisfactory performance in Phase 1.

Project Metrics:

The Project will measure success through a combination of metrics, co-designed with and approved by VA, which may include, but not limited to: 1) number of veterans recruited; 2) attendance to track retention and engagement; 3) tracking access to resources (and subsequently utilization); and 4) comparing outcomes between sites. A two-phased approach will be used and the REAIM framework shall be used to evaluate impact in both phases. Contractor shall engage 300 Veterans by end of Phase 1, and 1000 Veterans by the end of Phase 2.

The below provides an example of how metrics may be tracked using the REAIM framework:

Reach	<ul style="list-style-type: none"> Track number of Veterans enrolled and engaged with solution. Track number of enrollments by enrollment channel or site. Veteran demographics (age, sex, branch of service, tribal affiliation, etc.)
Effectiveness	<ul style="list-style-type: none"> Assess ability to reduce increase engagement through user feedback and participation rates. Track new connections to VHA resources via self-report
Adoption	<ul style="list-style-type: none"> Uptake of resources Track ease of use Track resource connection and/or referral engagement. Track enrolled Veterans Track number of text messages sent and responded to
Implementation	<ul style="list-style-type: none"> UX improvements made based on feedback. Ease of deployment with new Community/VA/VSO partners Feedback on ease of use Feedback on resource access, by mode of access, and referral process Evaluate effectiveness of resource provision Test and evaluate VA integration for closed loop referrals

Maintenance	<ul style="list-style-type: none"> • Success of operational integration for all MOU-connected partners • Successful development of long-term scaling and sustainability plan
-------------	--

3.2.1 PHASE 1: Prototyping/Testing

Phase 1 will include a proof-of-concept study to conduct a needs assessment of stakeholder prospects—rural Veteran Service Organizations (VSOs), VA staff, State & Tribal Veteran Agency—as well as the needs and barriers faced by end-users (Native & Women Veterans).

Phase 1 is necessary to create (a) a secure back-end data infrastructure with low-tech interfaces that are accessible (SMS text, phone access) for veteran engagement and (b) collect utilization, engagement, and goal fulfillment metrics which will become baseline metrics for Phase II: (a) iteratively improving the veteran user experience (front-end design) with low-tech veteran engagement infrastructure, and (b) validating a scalable model for the tribes and VA (access to resources, peer support training).

3.2.2 PHASE 2: Field Test/Pilot

Phase 2 will focus on expanding partnerships and engagement to additional tribes and other organizations/VA sites of care to further impact both AIANV and women Veterans. Deliverables will include HSP Iteration focused on developing culturally competent screening for needs assessment and intake for BRAVE Journeys and VTC integration of resource interfaces, developing low-tech interfaces for veteran engagement (Referral Information), and determining pathway for VA Integration for Closed Loop Referral, including providing VA staff (Case-management follow up) with direct data exchange and upgrading IT Cybersecurity for federal use.

3.3 INTENDED BENEFITS OF THE SOLUTION

Peer Support has proven to be valuable in many disciplines, complementing resource coordination and care, as well as reinforcing positive behaviors in Mental Health, Substance Use Disorder, Social Isolation, and Sexual Trauma. Current services utilize a one-size-fits-all approach, which increases the amount of work or energy required from unique populations like AI/AN, Veterans, women, and other at-risk populations to find the support and resources they need. This project streamlines the PS referral process with proprietary screening and complements veteran engagement via inclusive low-tech omni-channel options. By developing better screening for underserved populations and connecting them to PS, Televeda hopes to enable populations to access resources available to them before or when a critical need arises. The following provides a list of proposed benefits (not all-inclusive):

- Tailored Offering: Provides a relevant solution to address the care support gap for AIANVs and women Veterans by building trust and a means of educating Veterans about available VA and community resources.

- **Community Engagement:** HSP may be a way to build direct connection and trust amongst AIANV and the VA. Instead of asking AIANVs to travel to the VA sites (barrier), HSP is proposed as a method of meeting the veterans where they are as a supplement to VA services they may be eligible for. Beyond just Veteran engagement, HSP's framework includes best practices for recruiting tribal peer support specialists, Elders and Traditional Healers into the system. Research shows that the successful adoption and implementation of effective interventions is strong community-level engagement and trust in healthcare workers and healthcare systems.
- **Resource Coordination:** The problem VHA staff has consistently shared as a challenge is resource coordination. Staff seems to maintain printed resource flyers in binders, or when available online there is no centralized database to easily search and coordinate. Further these resources tend to get outdated fairly often due to budget cuts, workforce churn, funding reallocations, etc. This solution will provide low-tech, easily accessible means of learning more about available resources.
- **Rural Engagement:** The development of low-tech interfaces for veteran communication may reap benefits of scale across rural settings. The data suggests that increasing community-based and culturally-responsive services (protective factors) will help prevent suicide in our given population, as AIANVs primarily live in rural Reservation areas.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) is one 12-month Base, with optional tasks.

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

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

Under current definitions, five 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
Thanksgiving

Second Monday in October
Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR).

The bulk of the tasks under this PWS shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their proposal and as stated below:

1 N 1st Street
Suite 603
Phoenix, AZ 85004

4.3 TRAVEL

All travel requirements (including plans, agenda, itinerary, and dates) shall be pre-approved by the COR (subject to local policy procedures) at a minimum of seven (7) business days prior to the trip, unless otherwise coordinated with the COR, and is strictly on a cost reimbursable basis, in accordance with Federal Travel Regulations (FTR). See FAR 31.205-46 Travel Costs. Trip Reports shall be submitted to the COR within five business days after trip completion. Each contractor invoice shall include copies of ALL receipts that support the travel costs claimed in the invoice. General and Administrative expenses will not be reimbursed.

The Government anticipates travel under this effort to perform associated tasks, throughout the PoP. Include all travel costs in your firm-fixed price line items. These costs will be directly reimbursed by the Government.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 TECHNICAL KICKOFF MEETING

The Contractor shall hold a project kickoff meeting within ten days after contract award. This meeting should be held via teleconference and/or web meeting. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each specific task and deliverable. The Contractor shall specify date, virtual meeting information, agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes shall be provided to all attendees within three calendar days after the meeting. The Contractor shall invite the CO, Contract Specialist (CS), COR, VA Project Manager (PM), and any other attendees deemed necessary by the aforementioned VA personnel.

Deliverable:

- A. Project Kickoff Meeting Agenda
- B. Project Kickoff Meeting Minutes

5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall be in electronic form in Microsoft Word and Excel or Project formats. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

The plan should include detailed tasks and deliverables with specified duration, objective, approach, potential challenges and mitigation, plan for measuring success or outcomes, completion criteria, deliverables, and responsible organization.

Deliverable:

- A. Contractor Project Management Plan

5.1.3 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Excel or Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month.

The Monthly Progress Reports shall cover all work cumulatively completed during prior reporting periods, the current reporting period, and work planned for the subsequent reporting period, to include a summary of the progress made, project milestone schedule, challenges, successes, proposed changes, and next steps. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables, as applicable, and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall attend an up to weekly teleconference meeting, cadence to be determined by the VA Program Manager, to be held at a time convenient for both the government and the Contractor. The Contractor shall provide Teleconference Progress Meeting Minutes within two business days after the

teleconference meeting. The Contractor shall provide weekly emails with the progress, issues, and mitigations to the VA Program Manager and additional VA team members as designated by the VA PM. This team will be introduced in the kickoff meeting.

Deliverable:

- A. Cumulative Monthly Progress Report
- B. Teleconference Progress Meeting Minutes
- C. Email Weekly to BAA project management team

5.2 PHASE 1

5.2.1 COLLABORATION AGREEMENTS

The Contractor shall reach out to at least 30 tribes or VSO organizations, execute formal partnerships with a minimum of 10 Veteran Service Organizations or tribes, and sustain engagement with at least 3-5. Contractor shall establish Memorandums of Understanding (MOU) with all collaborating VSOs, tribes, and other supporting organizations or VA sites of care as needed, including any external organizations supporting evaluation, and provide a report on those established partnerships.

Deliverables:

- A. MOU Report

5.2.2 PROTOTYPE WIREFRAMING AND FOCUS GROUPS

Contractor shall update interface designs in HSP with 1) onboarding (intake), 2) culturally competent screening tool, 3) VTC programmatic display of resources and safety protocols, 4) HSP curriculum modification with resources. This will be completed through developing the wireframes of HSP user journey, screening and intake tool, VTC Suicide Prevention Safety Resources, and Stakeholder interviews completions for referrals and follow-up steps.

Contractor shall complete end-user focus groups with AIANV (rural and urban), women Veterans, and general population Veterans and will synthesize results to develop requirements and design specifications as part of proof-of-concept. Contractor shall collect data via participatory research with 30-50 Veterans, the VA, NNVA, AzDVS and AI/AN stakeholders to identify user needs and workflows for closed-loop referrals. As determined appropriately by MOU'd partners, Contractor shall gather needs-based data relating to SDOH screenings, including demographic information, and social factors. Contractor will also collect interest-driven proprietary data on users' recreational interests and socialization preferences from Televeda's social events platform. Contractor shall provide a User Journey Map and Focus Group Report to VA PM. This proof-of concept

data will establish a baseline for prototype development and evaluation to demonstrate the feasibility of our innovation.

Contractor shall work with VA PM, and additional VA team members as designated by PM, to modify existing screening tools to meet the specific needs, considering historical and cultural contexts, of AIANV and women Veterans. This shall be completed through stakeholder meetings, at least 10, to design a Service Blueprint, inclusive of Digital Navigators to track outcomes with follow-ups to verify appropriateness and resource utilization as well as determination of appropriate channels and personnel to send data to (what data is helpful, at what stage, process for dissemination & relevant stakeholders to inform). Contractor shall provide to the VA the final co-developed screening tool specific to subpopulations.

Deliverables:

- A. Functional Prototype of the B.R.A.V.E Journey in Peer Support for field testing
- B. Screening tool
- C. User Journey Map
- D. Focus Group Report

5.2.3 SUSTAINABLE DATA ACCESS AND ANALYSIS

Contractor shall coordinate with VA Program Manager to determine metrics associated with project goals and specify the means of capturing required information in a data collection and analytics plan. Data collection and analytics plan will also include co-development of Veteran survey questions or screening tools. Contractor shall provide aggregated, deidentified data showing impact of engagement including both quantitative and qualitative metrics as well as develop a means of completing and visualizing data analytics accessible by VA. Data should include, but not limited to, engagement and number of Veterans using solution, Veterans ratings of sessions, tracking of access to resources. Contractor shall use the REAIM evaluation framework to evaluate impact, value, and all associated processes and outcomes, in all phases of this project. Final plan, including metrics, shall be presented to the VA Program Manager for approval before developing a data analytics visualization solution.

The Contractor shall develop a means of accessing data metrics and analytics determined and approved by VA PM that will be accessible to both external partners and VA to enable joint, real-time monitoring of aggregate Veteran engagement and utilization of solution data.

Once Contractor has developed a resource for providing real-time data analytics visualization, VA PM must be provided access for review and approval. Resource may be tested and iterated upon in Phase 1 and Phase 2.

Deliverables:

Commented (b)(1); (b)(5)
(b)(5)

Commented (b)(1); (b)(5)
(b)(5)

- A. Data Collection and Analytics Plan
- B. Monthly Data Analysis Report
- C. Project Data Access Resource with Real-time Data Analytics Visualization

5.2.4 BASE RESOURCES COLLECTION AND COORDINATION PLAN

Contractor shall work with VA PM, or designated VA team, and external partners, including coordinating with tribal partners, social workers, case managers, to develop a base resources list for subpopulations and trauma-specific resource datasets, to test Contractor’s closed-loop tracking in Phase 2. Contractor shall also complete some limited resource integrations in their user interface and storytelling curriculum. Contractor shall develop a Resource Landscape Report, inclusive of sample specialty subpopulation resources for purposes of testing, and provide it to the VA PM for review and approval.

Contractor shall work with VA PM and other relevant stakeholders to develop a plan for resource coordination, including referrals, across identified Veteran subpopulations.

Deliverables:

- A. Resource Landscape Report
- B. Resource Coordination Plan

5.2.5 INTERFACE DEVELOPMENT AND RECRUITMENT STRATEGY

Contractor shall develop secure data collection endpoints for accessible Veteran user coordination and data exchange. Planned coordination, using developed endpoints, with the Veteran end users via Email, SMS Text, Phone Calls, or in-person (paper forms) for Outreach and Utilization monitoring shall be tested in Phase 2. Contractor shall provide a report detailing planning connection points using omni-channel options, such as SMS text bot, phone queries, and OCR tech for paper forms, inclusive of technical architecture for programmatic resource coordination for AIANV and women Veterans.

Contractor shall also develop a recruitment strategy, in collaboration with prior and new MOU’d partners, VA PM, and designated VA team members, Contractor shall provide to the VA PM a Recruitment Strategy Plan for approval.

Recruitment Strategy Plan shall be updated by Contractor in Phase 1 and Phase 2 for any newly added partners or tribes to ensure a culturally competent plan.

Deliverables:

- A. Engagement Interface Development and Testing Plan
- B. Recruitment Strategy Plan

5.2.6 USABILITY TESTING AND PRODUCT OR PROCESS ITERATION

Commented (b)(1); (b)(5)
(b)(5)

Commented (b)(6); (b)(5)
(b)(5)

Contractor shall utilize developed interfaces, Resource Coordination Plan, Data Collection Plan, and co-developed Screening tool to complete usability testing with both newly participating AIANV and women Veterans to ensure accurate capturing of cultural-specific contexts. Details of usability testing, including number of participants, to be co-determined with VA Program Manager. Contractor shall provide to VA a Usability Testing Plan. Once Usability testing is complete, Contractor shall provide to VA PM a Usability Testing Report including qualitative and quantitative data captured during testing from all participants and planned changes to product or process based on feedback.

Deliverables:

- A. Phase 1 Usability Testing Plan
- B. Phase 1 Usability Testing Report

5.2.7 FINAL PHASE 1 REPORT

At the completion of Phase 1, Contractor shall provide to the VA Program Manager a Phase Summary Report, inclusive of all work completed during Phase 1 and all data analytics required to meet project goals and determination of innovation value.

Deliverables:

- A. Final Phase 1 Summary Report

5.3 OPTIONAL TASK – PHASE 2

If VA exercises the Optional Task, the Contractor shall perform tasks identified in Sections 5.1 and all subsections, except 5.1.1. The period of performance for this optional task is 12 months. In reference to the deliverables in these sections, if the task has generated a document during the base period, the Contractor shall provide updates only. If VA exercises the Option Period, the Contractor shall also perform the following:

5.3.1 DATA COLLECTION AND ANALYSIS

Based on feedback in Phase 1, Contractor shall continue to work with VA PM to move forward with a making available a mechanism for VA employees to access data through secure channels. Contractor shall work with VA PM and other staff to iterate on the Mode of Real-time Data Analytics Visualization developed in Phase 1 and make it available to any newly participating stakeholders.

Contractor shall monitor metrics, co-determined in Phase 1 in the Data Collection Plan, and make data available to VA throughout Phase 2, to evaluate usability, engagement, and effectiveness. Contractor shall measure for an increase in retention and engagement from baseline. Contractor shall provide back to the VA PM monthly reports on engagement, access, and other key metrics, including user feedback, specific resource requests from platform communication channels, and testing results.

Commented (b)(5) 01: (b)(5)

(b)(5)

Commented (b)(6) 10: (b)(5)

(b)(5)

Commented (b)(6) 11: (b)(5)

(b)(5)

Commented (b)(6) 12: (b)(5)

(b)(5)

Deliverables:

- A. Monthly Data Analysis Reports

5.3.2 EXPANSION TO ADDITIONAL PARTNERS AND PEER SUPPORT SPECIALIST TRAINING

Contractor shall launch solution with at least an additional 3-5 tribes once formal partnerships supported by MOU are in place. If new MOUs or partnerships are added in Phase 2, an additional MOU report shall be provided by the Contractor to the VA PM.

Contractor shall develop an HSP Peer Support Training Module to equip Veteran peers with skills to facilitate HSP sessions. This module shall be developed, as needed, with VA subject matter expert support and in collaboration with all tribal and VSO partners. Module shall be provided to VA PM for review and approval. This training will be provided after each potential HSP Peer Support Specialist has obtained their state-approved Peer Support Specialist certification.

Contractor shall train a minimum of 10 Veteran peers by the end of Phase 2 and will develop a plan to use an Ambassador approach to recruiting additional peers to complete training and/or facilitate sessions. This plan for recruitment and facilitation shall be provided to the VA Program Manager for review and approval.

Deliverables:

- A. MOU Report
- B. HSP Peer Support Training Module
- C. Ambassador and Peer Support Recruitment and Facilitation Plan

5.2.8 ADDITIONAL RESOURCES COLLECTION

Contractor shall work with VA PM, or designated VA team, and external partners, including coordinating with tribal partners, social workers, case managers, to develop an updated resources list, inclusive of resources pertinent to newly added partners, tribes, or women Veteran subpopulations and trauma-specific resource datasets, to test Contractor's Resource Coordination Plan in Phase 2.

Contractor shall also complete some additional resource integrations in their user interface and storytelling curriculum. Contractor shall develop a Resource Landscape Report, inclusive of sample specialty subpopulation resources for purposes of testing and provide it to the VA PM for review and approval.

Contractor shall work with VA PM and other relevant stakeholders to implement and test the plan for resource coordination, including referrals, across identified Veteran subpopulations as part of Phase 2 Usability and Feasibility Testing.

Commented (b)(6) 41: (b)(5)
(b)(5)

Commented (b)(6) 41: (b)(5)
(b)(5)

Commented (b)(6) R14: (b)(5)
(b)(5)

Commented (b)(6) 41: (b)(5)
(b)(5)

Deliverables:

- C. Resource Landscape Report

5.3.3 USABILITY TESTING AND PRODUCT OR PROCESS ITERATION

Contractor shall utilize all developed interfaces, Resource Coordination Plan, Data Collection Plan, and co-developed Screening tool, and other developed plans and resources to complete additional usability testing with Phase 2 newly participating AIANV and women Veterans to ensure accurate capturing of cultural or tribal-specific contexts. Details of usability testing, including number of participants, to be co-determined with VA Program Manager. Contractor shall provide to VA a Usability Testing Plan. Once Usability testing is complete, Contractor shall provide to VA PM a Usability Testing Report, including qualitative and quantitative data captured during testing from all participants and planned changes to product or process based on feedback.

Deliverables:

- C. Phase 2 Usability Testing Plan
- D. Phase 2 Usability Testing Report

5.3.4 FEASIBILITY OF SCALE TESTING

Contractor shall develop a plan for feasibility of scale testing, beyond ongoing usability testing, and inclusive of new feasibility of scale metrics co-determined with VA that can be included in the Data Collection Plan. This plan shall be provided to VA PM for review and approval.

Contractor shall complete Feasibility of Scale Testing with at least 3-5 tribes, organizations, or VA sites in Phase 2, inclusive of deployment of all developed resources, interfaces, and means of data collection and visualization. Contractor shall provide a Feasibility Testing Report to VA PM.

Deliverables:

- A. Feasibility Testing Plan
- B. Feasibility Testing Report

5.3.5 OPERATIONAL PLAYBOOK FOR SCALABILITY

Based on results of all usability and feasibility testing, and with feedback and insights from all partners and VA, Contractor shall develop a uniform process via an Operational Playbook for Sustainability and Scalability for implementing the solution with additional partners in the future to be adaptable to any specific organization or tribe.

Deliverable:

A. Operational Playbook for Sustainability and Scalability

5.3.6 PHASE 1 AND PHASE 2 COMBINED FINAL REPORT

At the completion of Phase 2, Contractor shall provide to the VA Program Manager a Project Summary Report, inclusive of all work completed during Phase 1 and 2 and all data analytics (initial data analyses and final data analyses of all data captured during all periods of performance) required to meet project goals and determination of innovation value. Summary Report will also include detailing the process and outcomes (e.g., number of Veterans enrolled in solution from each source/site, etc.).

Deliverable:

- A. Phase 1 and Phase 2 Final Project Report

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

Not Applicable

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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:

Commented (b)(6) (b)(5)
 Commented (b)(6) (b)(5)
 (b)(5)

- 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. 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 PAL template artifact. 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.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
- d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed SIC Fingerprint Request Form
- e. 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).
- f. 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 e-QIP).
- g. 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.

- h. 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), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. 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 OPM.
- i. 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.
- j. 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.
- k. 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 Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none"> 1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none"> 1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems 	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none"> 1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks 	Satisfactory or higher
D. Management	<ol style="list-style-type: none"> 1. Integration and coordination of all activities to execute effort 	Satisfactory or higher

The COR 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 level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.5 FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will 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.

6.6 GOVERNMENT FURNISHED PROPERTY

Not Applicable

6.7 VHA National BAA Standard Language: It has been determined that protected health information (PHI) may be used, disclosed, accessed, transmitted, created, stored/maintained, and/or destroyed (providing appropriate proof of destruction in compliance with VA Directive 6371) by the Contractor, and a signed Business Associate Agreement (BAA) will be required. The Contractor will adhere to the requirements set forth within the BAA, referenced in the solicitation, and will comply with all applicable VA/VHA Directives. Once awarded, Contractor and Contracting Officer will collaborate with the VHA Privacy Office BAA team (b)(6) [@va.gov](mailto: @va.gov) to implement the appropriate National BAA.

Deliverable: Business Associate Agreement

(b)(5)

(b)(5)

(b)(5)

(b)(5)

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

1. **VA INFORMATION CUSTODIAL LANGUAGE.** This entire section applies to all acquisitions requiring any Information Security and Privacy language.
 - a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*. The primary clause used to define computer software license (not data/intellectual property first produced under this contractor or order) is FAR 52.227-19, *Commercial Computer Software License*.
 - b. Information made available to the contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*.
 - c. VA information will not be co-mingled with any other data on the contractor's information systems or media storage systems. The contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

- d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to contractor and subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.
- e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.
- f. The contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.
- g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.
- h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.
- i. The contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.
- j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.
- k. Notwithstanding the provision above, the contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality- assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of

certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the contractor is in receipt of a court order or other requests for the above- mentioned information, the contractor shall immediately refer such court order or other requests to the VA CO for response.

- I. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.
- li. Any data destruction done on behalf of VA by a contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.
- lii. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, *Guidelines for Media Sanitization* prior to termination or completion of this contract. If directed by the COR/CO, the contractor shall return all Federal Records to VA for disposition.
- liii. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.
- liv. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS. This section

applies when any person requires access to information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract.

- a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified

- in the solicitation or contract. This includes indirect entities, both affiliate of contractor/subcontractor and agent of contractor/subcontractor.
- b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.
 - c. All contractors and subcontractors working with VA information are subject to the same security investigative and clearance requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).
 - d. All contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All contractors and subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the contractor must state where all non-U.S. services are provided. The contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.
 - e. The contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
 - (1) Contractor/subcontractor personnel no longer has a need for access to VA information or VA information systems.
 - (6) Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.
 - (6) Contractor believes their own personnel or subcontractor personnel may pose a threat to their company's working environment or to any company- owned property. This includes contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

- (6) Any previously undisclosed changes to contractor/subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.
 - (6) Contractor/subcontractor personnel have their authorization to work in the United States revoked.
 - (6) Agreement by which contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for contractor personnel.
- f. In such cases of contract fulfillment, termination, or other causes; the contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by contractor/subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.
- g. Contractors/subcontractors who no longer require VA accesses will return VA- issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, contractors shall notify the appropriate VA COR/CO.
4. **TRAINING.** This entire section applies to all acquisitions which include section 3.
- a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:
 - (1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.
 - (3) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and
 - (3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role- based information security training].
 - b. The contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

- c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.
5. **SECURITY INCIDENT INVESTIGATION.** This entire section applies to all acquisitions requiring any Information Security and Privacy language.
- a. The contractor, subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the contractor, subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.
 - b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:
 - (6) The date and time (or approximation of) the Security Incident occurred.
 - (6) The names of individuals involved (when applicable).
 - (6) The physical and logical (if applicable) location of the incident.
 - (6) Why the Security Incident took place (i.e., catalyst for the failure).
 - (6) The amount of data belonging to VA believed to have been compromised.
 - (6) The remediation measures the contractor is taking to ensure no future incidents of a similar nature.
 - c. After the contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The contractor, subcontractor, and their employees 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.
 - ci. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.
 - cii. 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.
 - ciii. The contractor shall comply with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, which establishes the

breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

- civ. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.
- cv. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated damages to the VA as set forth in clause [852.211-76, Liquidated Damages— Reimbursement for Data Breach Costs](#).

6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT. This entire section

applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (to include the subcomponents of each) designed or developed for or on behalf of VA by any non-VA entity.

- a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).
- b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.
- c. VA IT contractors, subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, *Risk Management Framework for Cloud Computing Services* and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work through the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

- d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M- 22-18 (September 14, 2022). The term "software" includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The contractor shall provide a self- attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self- attestation.
- e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.
- f. The contractor shall ensure all contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.
- g. The contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository.
- h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default "program

files" directory with silently install and uninstall. The contractor shall perform testing of all updates and patching prior to implementation on VA systems.

- i. Applications designed for normal end users will run in the standard user context without elevated system administration privileges.
- j. The contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.
- k. The contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

- l. The Contractor shall comply with the Privacy Act of 1974 (the Act), FAR 52.224- 2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.
- li. The contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as "Information Systems") throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The contractor shall ensure security fixes do not negatively impact the Information Systems.
- lii. When the contractor is responsible for operations or maintenance of the systems, the contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE.

This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (cloud and non- cloud) hosted, operated, maintained, or used on behalf of VA at non-VA facilities.

- a. The contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security

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

- b. Outsourcing (contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.
- c. The contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.
- ci. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).
- cii. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with contractor activities are also subject to such assessments. The contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.
- ciii. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required

to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

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

- h. VA prohibits the installation and use of personally owned or contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved contractor OE will be subject to technical inspection at any time.
- i. The contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.
- j. For cases wherein the contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.
- k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity &

Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22- 01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT

AND AUDITING. This entire section applies whenever section 6 or 7 is included.

- a. Should VA request it, the contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the contractor's IT or systems and controls, to ascertain whether the contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the contractor.
- b. Any audits or tests of the contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the contractor uses to destroy, maintain, receive, retain, or use VA information.
- c. As part of these audits, tests and assessments, the contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.
- d. The contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the contractor has generated as part of its own security assessment. The contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.
- e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT

AND ANTI-TAMPERING. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.

- a. The contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain", which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.
- b. When contracting terms require the contractor to procure equipment, the contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.
- c. All contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The contractor shall make spare parts available. All contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The contractor shall apply encryption technology to protect procured products throughout the delivery process.
- d. If a contractor provides software or patches to VA, the contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).
- e. The contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report "The Minimum Elements for a Software Bill of Materials (SBOM)."
- f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.
- g. Throughout the delivery process, the contractor shall demonstrate a capability for detecting unauthorized access (tampering).
- h. The contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

10. **VIRUSES, FIRMWARE AND MALWARE.** This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.
- a. The contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.
 - b. The contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.
 - c. The contractor shall provide or arrange for the provision of technical justification as to why any "false positive" hit has taken place to ensure their code's supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.
 - d. The contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter "virus or other malware") onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the contractor shall:
 - (2) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA's information networks, computer systems and information systems; and
 - (2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.
11. **CRYPTOGRAPHIC REQUIREMENT.** This entire section applies whenever the acquisition includes section 6 or 7 is included.
- a. The contractor shall document how the cryptographic system supporting the contractor's products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.
 - b. The contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.
 - c. The contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

- d. The contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.
- e. The contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

12. PATCHING GOVERNANCE. This entire section applies whenever the acquisition includes section 7 is included

- a. The contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the follow:
 - (2) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and
 - (2) The approach and capability to remediate newly reported zero-day vulnerabilities for contractor products.
- b. The contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.
- c. The contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by contractor within these time periods, the contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.
- d. The contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE

SYSTEMS, RESEARCH SCIENTIFIC COMPUTING). This entire section applies when the acquisition includes one or more Medical Device, Special Purpose System or Research Scientific Computing Device. If appropriate, ensure selected clauses from section 6 or 7 and 8 through 12 are included.

- a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing

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

- b. All contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work through the COR/CO for governance or resolution.
- c. The contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.
- d. The contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Postmarket Management of Cybersecurity in Medical Devices.

- e. The contractor shall design devices capable of accepting all applicable security patches with or without the support of the contractor personnel. If patching can only be completed by the contractor, the contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.
- f. The contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the contractor cannot install an anti-virus / anti-malware application.
- g. The contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.

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

- (3) The contractor shall accept the system without the drive, firmware and solid state.
- (3) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or
- (3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:
 - (b) The equipment contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.
 - (b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

- 14. **DATA CENTER PROVISIONS.** This entire section applies whenever the acquisition requires an interconnection to/from the VA network to/from a non-VA location.
 - a. The contractor shall ensure the VA network is accessed by in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.
 - b. The contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.
 - c. The contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).
 - d. The contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.
 - e. The contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.
 - f. The contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA

Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

SECTION C - CONTRACT CLAUSES

C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (JAN 2017)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights—

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

Notwithstanding the foregoing, use of the item in production will constitute acceptance by the VA.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions*. The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include—

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer—System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity.* The Contractor shall indemnify the Government 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 the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payment.—

(1) *Items accepted.* Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) *Electronic Funds Transfer (EFT).* If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount.* In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments.* If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) *Interest.*

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) *Final decisions.* The Contracting Officer will issue a final decision as required by 33.211 if—

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss.* Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes.* The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience.* The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title.* Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty.* The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability.* Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances.* The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments

(9) The specification.

(t) *System for Award Management (SAM).*

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the SAM database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the SAM database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the SAM database to ensure it is current, accurate and complete. Updating information in the SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in FAR subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the SAM database; (B) comply with the requirements of subpart 42.12; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the SAM database. Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via SAM accessed through <https://www.acquisition.gov>.

(u) *Unauthorized Obligations.*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA),

Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government 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:

(i) Any such clause is unenforceable against the Government.

(ii) 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 EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or 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.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference.* The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of Clause)

**ADDENDUM to FAR 52.212-4 CONTRACT TERMS AND CONDITIONS—
COMMERCIAL ITEMS**

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

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

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

<http://www.acquisition.gov/far/index.html>
<http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm>

<u>FAR</u>	<u>Title</u>	<u>Date</u>
<u>Number</u>		

52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION)	FEB 2015
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	MAY 2011
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE	JUL 2016
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	OCT 2014
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-14	RIGHTS IN DATA—GENERAL	MAY 2014
52.227-17	RIGHTS IN DATA—SPECIAL WORKS	DEC 2007
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	DEC 2013

(End of Clause)

C.3 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

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

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements and procedures.* (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of Clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 24 months.

(End of Clause)

C.5 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.6 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

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

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

(2) *Designated agency office* has the meaning given in 5 CFR 1315.2(m).

(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.

(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. (See Web site at <http://www.fsc.va.gov/einvoice.asp>.)

(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). The X12 EDI Web site (<http://www.x12.org>) includes additional information on EDI 810 and 811 formats.

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

(e) *Exceptions*. If, based on one of the circumstances below, 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)

C.7 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of the state in which the majority of the work will take place. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.8 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

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 shall be furnished to the contractor.

(End of Clause)

C.9 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(3) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(4) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

(4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (OCT 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

(6) 52.204-14, Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

(7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

(8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (OCT 2015) (31 U.S.C. 6101 note).

(9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

(10) [Reserved]

(11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

(ii) Alternate I (NOV 2011) of 52.219-3.

(12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

(ii) Alternate I (JAN 2011) of 52.219-4.

(13) [Reserved]

(14)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

(ii) Alternate I (NOV 2011).

(iii) Alternate II (NOV 2011).

(15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

(ii) Alternate I (Oct 1995) of 52.219-7.

(iii) Alternate II (Mar 2004) of 52.219-7.

(16) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)).

(17)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2017) (15 U.S.C. 637(d)(4)).

(ii) Alternate I (NOV 2016) of 52.219-9.

(iii) Alternate II (NOV 2016) of 52.219-9.

(iv) Alternate III (NOV 2016) of 52.219-9.

(v) Alternate IV (NOV 2016) of 52.219-9.

(18) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

(19) 52.219-14, Limitations on Subcontracting (JAN 2017) (15 U.S.C. 637(a)(14)).

(20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

(22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).

(23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (DEC 2015) (15 U.S.C. 637(m)).

(24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015) (15 U.S.C. 637(m)).

(25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

(26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (JAN 2018) (E.O. 13126).

(27) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(28) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(29) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(30) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(31) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

(32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

(33)(i) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(ii) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(34) 52.222-54, Employment Eligibility Verification (OCT 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

(35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

(ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

(36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).

(37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).

(38)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).

(ii) Alternate I (OCT 2015) of 52.223-13.

(39)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).

(ii) Alternate I (JUN 2014) of 52.223-14.

(40) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

(41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).

(ii) Alternate I (JUN 2014) of 52.223-16.

(42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)

(43) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).

(44) 52.223-21, Foams (JUN 2016) (E.O. 13693).

(45) (i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(ii) Alternate I (JAN 2017) of 52.224-3.

(46) 52.225-1, Buy American—Supplies (MAY 2014) (41 U.S.C. chapter 83).

(47)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

(ii) Alternate I (MAY 2014) of 52.225-3.

(iii) Alternate II (MAY 2014) of 52.225-3.

(iv) Alternate III (MAY 2014) of 52.225-3.

(48) 52.225-5, Trade Agreements (OCT 2016) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

(49) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

(50) 52.225–26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

(52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

(53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

(54) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

(55) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013) (31 U.S.C. 3332).

(56) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

(57) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

(58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

(59) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(12)).

(60)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

(ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495).

(2) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(3) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[] (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[] (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[] (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

[] (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

[] (8) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

[] (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

[] (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792).

[] (11) 52.237-11, Accepting and Dispensing of \$1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not

require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities.

(iv) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(v) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(vi) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(vii) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(viii) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(ix) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

(x) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(xii)(A) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xv) 52.222-54, Employment Eligibility Verification (OCT 2015) (E. O. 12989).

(xvi) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

(xvii) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xviii)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(B) Alternate I (JAN 2017) of 52.224-3.

(xix) 52.225–26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xx) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

VA118-15-R-0074

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

D.1 - Business Associate Agreement.

**PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Veteran's Health Administration (VHA)
VHA Innovation Ecosystem (14HIL1)**

Virtual Reality (VR) for Suicide Prevention Training

**Date: 10 February 2025
PWS Version Number: 1.5**

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS3

- B.1 GOVERNING LAW3
- B.2 CONTRACT ADMINISTRATION DATA4
- B.3 PRICE SCHEDULE5
- B.4 PERFORMANCE WORK STATEMENT12

SECTION C - CONTRACT CLAUSES59

- C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (JAN 2017)59
- C.2 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998).....66
- C.3 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)67
- C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) ...69
- C.5 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)69
- C.6 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)69
- C.7 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)71
- C.8 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)71
- C.9 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)71

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS\.....80

- D.1 Business Associate Agreement.....54

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations ("FAR"), shall govern this Order. Commercial license agreements may be made a part of this Order but only if both parties expressly make them an addendum. 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 Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap) or 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 Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this 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 Order. Federal law and regulation, including without limitation, the Contract Disputes Act (41 U.S.C. §601-613), the Anti-Deficiency Act (31 U.S.C. §1341 et seq.), the Competition in Contracting Act (41 U.S.C. §253), the Prompt Payment Act (31 U.S.C. §3901, et seq.) and FAR clauses 52.212-4, 52.227-14, 52.227-19 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 Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 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 Order must be made by order modification (Standard Form 30). Nothing in this Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.2 CONTRACT ADMINISTRATION DATA

(continuation from Standard Form 1449, block 18A.)

1. CONTRACT ADMINISTRATION: All contract administration matters will be handled by the following individuals:

- a. CONTRACTOR: **Customer** Value Partners, LLC
 805 Fifteenth St, Suite 650
 Washington, D.C. 20005
 CAGE: 3EU68
 UEI: L6R3M86AFBB5

 Technical POC:
 (b)(6)
 Vice President, Contracts
 805 Fifteenth St, Suite 650
 Washington, D.C. 20005
 703-345-(b)(6)@cvpcorp.com
- b. GOVERNMENT: Contracting Officer 36C10B
 Attn: Jamie Bennett, Contracting Officer
 Department of Veterans Affairs
 Technology Acquisition Center
 23 Christopher Way
 Eatontown NJ 07724

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

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: upon receipt of deliverables
 - a. Quarterly
 - b. Semi-Annually
 - c. Other Upon acceptance of deliverables in accordance with B.3 Price Schedule

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.

B.3 PRICE SCHEDULE (this will be completed AFTER Section 5 is completed)

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

BASE PERIOD					
LINE ITEM	DELIVERABLE	QTY	UNIT	UNIT PRICE	TOTAL
0001	<p>Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs.</p> <p>This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, project management, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs.</p> <p>Period of Performance (PoP) shall be September 30, 2018 – September 29, 2019.</p> <p>Electronic submission to: VA Program Manager (PM), Contracting Officer Representative (COR) and Contracting Officer (CO).</p> <p>Inspection: destination Acceptance: destination</p>	12	MO	Not Separately Priced (NSP)	NSP
0001AA	<p>Project Kickoff Meeting Agenda IAW PWS Paragraph 5.1.1</p> <p>Due: Five days prior to the Technical Kickoff Meeting.</p>	1	EA	NSP	NSP
0001AB	<p>Project Kickoff Meeting Minutes IAW PWS Paragraph 5.1.1</p> <p>Due: Three days after the Technical Kickoff Meeting</p>	1	EA	NSP	NSP

0001AC	Contractor Project Management Plan IAW PWS Paragraph 5.1.2 Due 30 days after contract (DAC) award and updated monthly thereafter	1	LO	NSP	NSP
0001AD	Monthly Progress Report IAW PWS Paragraph 5.1.3 Due on the fifth day of each month throughout the PoP.	1	LO	NSP	NSP
0001AE	Teleconference Progress Meeting Minutes IAW PWS Paragraph 5.1.3 Due two days after the Teleconference Progress Meetings	1	LO	NSP	NSP
0001AF	Collaboration Agreements from VA/and VSO PWS Paragraph 5.1.4 Due 30 DAC award	1	EA	NSP	NSP
0001AG	Paragraph 5.1.4 Due 30 DAC award	1	EA	NSP	NSP
0001AH	Contractor Staff Roster IAW PWS Paragraph 6.2.2 Due 3 DAC award and updated within one day of any changes in employee status.	1	EA	NSP	NSP
0002	Initial Phase shall be provided IAW PWS Paragraph 5.2, and all of its subparagraphs. This FFP CLIN includes all labor, materials, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.2, inclusive of all subparagraphs. Period of Performance (PoP) shall be September 30, 2018 – September 29, 2019.	1	LO	NSP	NSP

	Electronic submission to: VA PM, COR and CO. Inspection: destination Acceptance: destination				
0002AA	IAW PWS paragraph 5.2.2 Due 30 after	1	EA		
0002AB	IAW PWS paragraph 5.2.2 Due 30 days after completion of Interviews	1	EA		
0002AC	Usability Testing Results IAW PWS paragraph 5.2.2 Due 30 days after completion of Usability Testing	1	EA		
0002AD	IAW PWS paragraph 5.2.2 Due 30 days after completion of Interviews	1	EA		
0002AE	IAW PWS paragraph 5.2.1 Due 120 DAC award	1	EA		
0002AF	IAW PWS paragraph 5.2.1 Due 120 DAC award	1	EA		
0002AG	Year 1 Final Report IAW PWS paragraph 5.2.3 Due 360 DAC award	1	EA		
TOTAL BASE PERIOD					
OPTION PERIOD ONE					
This Option may be exercised in accordance with FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer					
LINE ITEM	DELIVERABLE	QTY	UNIT	UNIT PRICE	TOTAL
1001	Project Management shall be provided IAW PWS Paragraph 5.1, and all of its subparagraphs, except 5.1.1. This FFP CLIN includes all labor, materials, and deliverables required for the successful completion of the services detailed in PWS	12	MO	Not Separately Priced (NSP)	NSP

	<p>Paragraph 5.1 and 6.2.2, inclusive of all subparagraphs..</p> <p>The PoP shall be 12-months commencing immediately upon expiration of the Base Period.</p> <p>Electronic submission to: VA Program Manager (PM), Contracting Officer Representative (COR) and Contracting Officer (CO).</p> <p>Inspection: destination Acceptance: destination</p> <p>The cost of CLIN 1001 shall be included in and allocated to CLINs 1002.</p>				
1001AA	<p>Contractor Project Management Plan IAW PWS Paragraph 5.1.2</p> <p>Due 30 days after commencement of Option and updated monthly thereafter</p>	1	LO	NSP	NSP
1001AB	<p>Monthly Progress Report IAW PWS Paragraph 5.1.3</p> <p>Due on the fifth day of each month throughout the PoP.</p>	1	LO	NSP	NSP
1001AC	<p>Teleconference Progress Meeting Minutes IAW PWS Paragraph 5.1.3</p> <p>Due two days after the Teleconference Progress Meetings</p>	1	LO	NSP	NSP
1001AD	<p>IAW PWS Paragraph 5.1.4</p> <p>Due 30 days after commencement of Option</p>	1	EA	NSP	NSP
1001AE	<p>IAW PWS Paragraph 5.1.4</p> <p>Due 30 days after commencement of Option</p>	1	EA	NSP	NSP
0001AF	<p>Contractor Staff Roster IAW PWS Paragraph 6.2.2</p>	1	EA	NSP	NSP

	Due within one day of any changes in employee status.				
	<p>Pilot Study shall be provided IAW PWS Paragraph 5.3, and all of its subparagraphs.</p> <p>This FFP CLIN includes all labor, materials, and deliverables required for the successful completion of the services detailed in PWS Paragraph 5.3, inclusive of all subparagraphs.</p> <p>The PoP shall be 12-months commencing immediately upon expiration of the Base Period</p> <p>Electronic submission to: VA PM, COR and CO.</p>				
1002	<p>Inspection: destination</p> <p>Acceptance: destination</p>	1	LO	NSP	NSP
1002AA	<p>Site-Specific Pilot Study Implementation Plans IAW PWS paragraph 5.3.1.1</p> <p>Due 90 days after commencement of Option Period</p>	1	EA		
1002AB	<p>IAW PWS paragraph 5.3.1.2</p> <p>Due 240 days after commencement of Option</p>	1	EA		
1002AC	<p>IAW PWS paragraph 5.3.1.2</p> <p>Due 240 days after commencement of Option</p>	1	EA		
1002AD	<p>Year 2 Final Report IAW PWS paragraph 5.3.1.3</p> <p>Due 360 days after commencement of Option</p>	1	EA		
TOTAL BASE PERIOD					
TOTAL AMOUNT (BASE + OPTION PERIOD)					
CLIN	Deliverable	Quantity	Unit	Unit Price	Total price

Commented (b)(1);(b)(5)
(b)(5)

0001	A. Immersive Technology for Suicide Prevention Training Monthly Progress Report	12.00	EA		NSP
0001a	Senior Software Engineer	480	HR	(b)(4)	
0001b	Instructional Training Designer	32	HR		
0001c	Junior Software Engineer	760	HR		
0001d	Immersive Artist	580	HR		
0002	B. Immersive Technology for Suicide Prevention Training Design File	1.00	EA		
0003	C. End-User Feedback Report (FFP)	8.00	EA		
0004	A. Prototype Evaluation Meeting Agenda	1.00	EA		
0005	B. Prototype Evaluating Meeting Minutes	1.00	EA		
0006	C. Prototype Evaluation Meeting Materials (e.g. PowerPoint presentations and any other handouts)	1.00	EA	(b)(4)	
0007	A. Pilot Evaluation Plan to include Prototype Experience for Suicide Prevention Training, Pilot testing checklist and End-User Feedback Report	8.00	EA		
0008	B. Pilot Benefits and Impact Report	14.00	EA		
0009	Other Direct Costs Not to Exceed (NTE)	1.00	LT		
0010	VR Equipment	4.00	EA		

Commented (b)(6); (b)(5)
(b)(5)

0011	TRAVEL NTE	1.00	LT	(b)(4)	
BASE PERIOD TOTAL					\$ 1,169,688.80
1001	A. Immersive Technology for Suicide Prevention Training Monthly Progress Report	12.00	EA	(b)(4)	
1001a	Senior Software Engineer	480	HR		
1001b	Instructional Training Designer	160	HR		
1001c	Junior Software Engineer	720	HR		
1001d	Immersive Artist	720	HR		
1002	B. Immersive Technology for Suicide Prevention Training Design File	1.00	EA		
1003	C. End-User Feedback Report (FFP)	8	EA		
1004	A. Prototype Evaluation Meeting Agenda	1.00	EA	(b)(4)	
1005	B. Prototype Evaluating Meeting Minutes	1.00	EA		
1006	C. Prototype Evaluation Meeting Materials (e.g. PowerPoint presentations and any other handouts)	1.00	EA		
1007	A. Pilot Evaluation Plan to include Prototype Experience for Suicide Prevention Training, Pilot testing checklist and End-User Feedback Report	8	EA		
1008	B. Pilot Benefits and Impact Report	14.00	EA		
1009	Other Direct Costs Not to Exceed (NTE)	1.00	LT		
1010	TRAVEL NTE	1.00	LT		
OPTION PERIOD 1 TOTAL					(b)(4)

B.4 PERFORMANCE WORK STATEMENT

Commented [b)(1)]: (b)(5)



**PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Veteran's Health Administration (VHA)
VHA Innovation Ecosystem (14HIL1)**

Virtual Reality (VR) for Suicide Prevention Training

**Date: 12 December 2024
TAC- 15-
PWS Version Number: 1.5**

1.0 BACKGROUND

As an innovation engine within the Department of Veterans Affairs, the vision of the Veterans Health Administration's Innovation Ecosystem (VHAIE) is a VA continuously innovating at the forefront of science and research, service delivery and implementation of solutions, and employee empowerment. VHAIE leads this vision by fostering organizational capability, delivering operational and clinical breakthroughs, and driving futures. VHAIE is committed to developing and employing agile mechanisms that allow VA to source incremental and transformational innovations to best serve Veterans and their families.

This Broad Agency Announcement (BAA) opportunity seeks to source and fund early-stage research, development, prototyping, field testing, and implementation piloting with an overall goal of moving forward the state of the art.

Through this BAA, VHAIE invites all potential offerors (including private sector companies, non-profits, and institutions of higher learning) to contribute ideas for innovations in SUICIDE prevention, care coordination, and treatment that significantly increase Veteran access to services, reduce or control costs of delivering those services, enhance the performance of VA operations, and improve the quality of service that Veterans and their families receive.

The significant and unprecedented challenges this country faced in 2021 fuel the continued call to action related to a whole-of-government and whole-of-nation approach to suicide prevention. Suicide is a complex problem requiring a full public health approach involving community prevention and clinical intervention. VA services are a critical part of this public health approach.

The data spanning 20 years reveals that Veterans engaged in VHA care have shown a less sharp rise in suicide rates, underscoring the importance of VHA care. Over 20 years of Veteran suicide data also reveal a substantial reduction in suicide rates, specifically for Recent Veteran VHA Users with mental health or substance use disorder diagnoses (77.8 per 100,000 in 2001 to 58.2 per 100,000 in 2021), falling 32.9% for Veterans with depression, 27.6% for those with posttraumatic stress disorder, 26.9% for those with anxiety and 40.4% for those with sedative use disorder. Comparing Veterans with Recent VHA use to other Veterans, we also find notable trends. While overall rates of Veteran suicide rose across the 20 years, age-adjusted suicide rates rose 24.5% for male Veterans with Recent VHA use compared to 62.6% for male Veterans without Recent VHA use. While less notable for women Veterans, the age-adjusted suicide rates rose 87.1% for female Veterans with Recent VHA use and 93.7% for female Veterans without Recent VHA use. Likewise, when looking more specifically across 2020 and 2021, we find the greatest increase in unadjusted rates for Veterans who were neither engaged with VHA nor with VBA. From 2020 to 2021, there were also notable decreases for particular subpopulations of Veterans with Recent VHA use, including those between ages 55- and 74-years-old (overall suicide rate -2.2%, -0.6% for men, -24.9% for women), males between ages 18- and

34-years-old (overall suicide rate -1.9%) and males aged 75-years-old and older (overall suicide rate -8.6%). These findings underscore the importance of continuing to expand access to and engagement of Veterans in VHA and VBA services, as over 50% of Veterans who died by suicide in 2021 had not been engaged in either service. Yet, in order to address the complex interweaving of individual, relational, community and societal risks, VA must continue to fully engage with other federal agencies; public-private partnerships; government at the local, state and 32 As noted above, Veterans receiving VHA care show evidence of higher risk with being more likely to have lower annual incomes, poorer self-reported health status, more chronic medical conditions, and self-reported disability due to physical or mental health factors, greater depression and anxiety, and greater reporting of trauma, lifetime psychopathology, and current suicidality. 10 national levels; VSOs; and local communities to reach all Veterans to support the implementation of a full public health approach, as outlined in the White House Strategy Reducing Military and Veteran Suicide (2021) 33 and VA's National Strategy for Preventing Veteran Suicide (2018). 34 These guiding documents have been operationalized through SP 2.0; Suicide Prevention Now initiative (SP Now); new laws, including the 2020 Commander John Scott Hannon Veterans Mental Health Care Improvement Act; the Veterans Comprehensive Prevention, Access to Care and Treatment Act (COMPACT) of 2020; the National Suicide Hotline Designation Act of 2020; and emerging innovations combined with research and program evaluation. As 2021 has again shown, this public health approach must include both community-based prevention and clinical interventions to reduce suicide in the Veteran population. As we reflect on the core of what we learned about Veteran suicide in 2021, 7 themes emerge for our call to action (see summary listing and description below). While no one solution can address the complexity of all factors involved in suicide, the data clearly outlines that significant reductions in Veteran suicide will not occur without meaningful focused effort to address Veteran firearm suicide. While we vigorously pursue enhanced policies, research, and programs to effectively address the broader socioecological and individual risk and protective factors which speak to "why" a Veteran may consider suicide, we must address directly the "how" of Veteran suicide. It is inescapable that the "how" in 72% of Veteran suicide deaths is firearm compared to 52% of non-Veteran U.S. adult suicides.

VHAIE, therefore, begins our call to action with a focus on primary topic areas that take into account the many facets of suicide prevention, including topics like the "how" of suicide, the importance of a community-led approach to preventing suicide, improved training, or increased access to care. To address the need for innovation in Suicide Prevention, VA seeks innovations across 7 primary topic areas:

- Promote firearm secure storage for Veteran suicide prevention.
- Implement and sustain community collaborations focused upon community-specific Veteran suicide prevention plans.
- Continue expansion of readily accessible crisis intervention services.

- Improve tailoring of prevention and intervention services to the needs, issues, and resources unique to Veteran subpopulations.
- Advance suicide prevention meaningfully into non-clinical support and intervention services, including financial, occupational, legal, and social domains.
- Increase access to and utilization of mental health across a full continuum of care.
- Integrate suicide prevention within medical settings to reach all Veterans.

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 Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules"
2. 10 U.S.C. § 2224, "Defense Information Assurance Program"
3. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
8. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
16. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
17. VA Handbook 6500.6, "Contract Security," March 12, 2010
18. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
19. OI&T Process Asset Library (PAL), <https://www.va.gov/process/>. Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp> NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
20. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015

Commented (b)(6); (b)(5)

21. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
22. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
23. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
24. 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
25. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
26. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
27. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
28. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
29. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
30. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
31. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
32. 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>)
33. 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>))
34. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
35. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
36. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
37. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
38. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
39. [The Veteran Metrics Initiative Well-Being Inventory, https://www.ptsd.va.gov/professional/assessment/documents/WellBeingAssessment.pdf](https://www.ptsd.va.gov/professional/assessment/documents/WellBeingAssessment.pdf)

3.0 SCOPE OF WORK

This contract and proposed solution focus on the following topic:

- Integrate suicide prevention within medical settings to reach all Veterans.

Topic Detail: Our data again showed that a significant percentage of VHA Veterans who died by suicide did not have a VHA mental health or substance use disorder diagnosis. We need to creatively address the needs of those at risk who may never seek mental health services and who may have other risk factors outside of mental health (e.g., pain, cancer, sleep disturbance) through expansion of suicide screening, assessment, and safety planning into all medical settings, within VHA and within community care.

3.1 Specific Problem to Address with this Solution:

The 2023 National Veteran Suicide Prevention Annual Report reveals that 6,392 Veterans died by suicide in 2021, an increase of 114 from the previous year. Suicide is a national healthcare concern, with Veterans facing higher rates than civilians. Many non-mental health staff lack proper training to recognize suicide warning signs. Traditional training methods, often using role-playing exercises, have proven ineffective, with participants reporting them as unrealistic and awkward. This poses a challenge in preparing healthcare providers to identify and address suicide risk effectively.

3.2 Proposed Solution:

The contractor shall design, develop, test, and validate a virtual, immersive environment that enables training related to the Suicide Prevention for VA employees. Work will include the development of a working prototype – including functionality across multiple head-mounted displays– to validate the virtual and immersive experience, done so in collaboration with VA clinical experts who will determine utility and feasibility of this solution.

The required outcomes for the proposed Immersive Technology solution are:

1. Customizable experiences considerate of factors related to social determinants of health, geographic region, and appropriate suicide prevention-related considerations
2. Hardware and software compatibility capable of screen-casting, both eye-gaze and hand controller manipulation, embedded data collection (such as, but not limited to, perceptions of the immersive experience, pre- and post-assessments, etc.)
3. Functionality for individual and/or group education and training sessions
4. Leverage Immersive Technology to advance the utilization of augmented, mixed, or virtual reality as a tool for VA employee training related to prevention of suicide.
5. Provide a more distributive and virtual experience, by which a VA employee and/or patient, in concert with clinical staff as appropriate, may utilize the technology, without having to be physically present at a VA facility.

The proposed solution is intended to empower VA practitioners to recognize suicidality signs and determine necessary actions, regardless of who the Veteran sees. Contractor plans to accomplish this by creating immersive and personalized training that goes beyond traditional methods, combining virtual reality with live, one-on-one coaching with Artificial Intelligence (AI). The solution will provide this hands-on practice in speaking with and identifying suicide risk in a safe, realistic environment.

The Project will use a human-centered design approach, including iterative processes, beginning with extensive user research, rapid prototyping, and then rigorous user testing. This cycle of prototyping, testing, and refining is repeated, incorporating immersive artwork to enhance authenticity and achieve maximum immersion.

To transform how healthcare providers identify and intervene in potential suicide risk scenarios, Contractor shall complete a pilot that includes the following:

1. Develop the VR training application.
2. Recruit 100 VA licensed medical providers.
3. Administer a pre-test survey on preparedness for dealing with suicidal ideation.
4. Assign 50 providers to a control group and 50 to receive our VR training.
5. After 8 weeks, conduct a post-test survey on preparedness and VR technique application and compare the results.

For this suicide prevention training program, Contractor will develop the front-end using the Unity IDE, a platform they have successfully utilized in creating other immersive applications for the VA. Contractor shall also develop an alternative version ("build") of the software that will run on a computer. While the computer-based version would provide a 2D experience rather than the immersive 3D environment of VR, it would still deliver the core training content and interactive elements. Contractor will deploy the app on Meta Quest headsets or a similar product approved by VA.

Contractor shall use a development process that integrates Agile methodologies with HCD principles. Contractor will conduct informational interviews with VA SMEs, collaborate closely with stakeholders, and involve VA PM and associated project team in frequent reviews. This approach ensures that the solution remains focused on end-user needs and aligns with VA objectives. Contractor will host the system's back-end in a secure AWS cloud environment, leveraging AI capabilities to assess learner progress in real-time. By using a large language model (LLM) for real-time evaluation against an expert-designed rubric, solution will provide personalized feedback based on VA-recommended practices. Contractor team shall adhere to secure coding practices throughout the development lifecycle, storing code in GitHub and other assets in a dedicated AWS account. Solution will utilize an auto-update capability to ensure ease of pushing new content or iterations to devices.

Solution may be designed with specific special Veteran populations as identified in the Annual Report.

3.2.1 Project Metrics:

The Project will measure success through a combination of metrics, co-designed with and approved by VA. A two-phased approach will be used, inclusive of a prototyping phase and then a field-testing phase. The REAIM

framework shall be used to evaluate impact in both phases. The below provides an example of how metrics may be tracked using the REAIM framework:

Reach	<ul style="list-style-type: none"> Track number of user testing and field testing participants Track pertinent aggregate information about participants such as clinical discipline, site, years of experience, or prior immersive experience. <ul style="list-style-type: none"> Track number of sites participating and number of end users providing feedback at each
Effectiveness	<ul style="list-style-type: none"> Assess and compare baseline knowledge and post-training knowledge Assess for any differences between traditional training and VR-based training Assess realism and sense of presence Assess accuracy of training based on existing curriculum and trainings
Adoption	<ul style="list-style-type: none"> Track ease of use (e.g. System Usability Scale) Track incidence of side effects <ul style="list-style-type: none"> Track number of participants and number of sites Track number of headsets being utilized and cost associated
Implementation	<ul style="list-style-type: none"> Track UX improvements made based on feedback. <ul style="list-style-type: none"> Feedback on ease of use Evaluate needed workflows for integration of training into current practices Evaluate value of mobility of solution Test and evaluate solution compared to standard
Maintenance	<ul style="list-style-type: none"> Evaluate perception of operational integration of solution into existing practices and systems including starting process of solution integration into VA systems if appropriate Successful development of long-term scaling and sustainability plan for solution

3.2.2 PHASE 1: Prototyping/Testing

Phase 1 (initial 12 months) shall focus on initial prototype development, including conducting informational interviews with VA SMEs, collaborating closely with stakeholders, and involving VA PM and associated project team in frequent reviews as prototype development progresses following an agile development process. Phase 1 will also include extensive user testing to gather feedback and iteratively refine the solution. Contractor shall work with VA PM and other VA Subject Matter Experts to determine which pre-existing curriculum(s) shall be used to develop the solution as well as primary training focus of the prototype solution.

During this phase, Contractor will work with VA experts to:

1. Identify key learning objectives and essential skills to be translated into the VR format

2. Develop realistic scenarios that align with these objectives
3. Structure the curriculum to best support the desired learning outcomes
4. Design interactive exercises that reinforce critical information and skills

Phase 1 will also include development of an Artificial Intelligence grading system to grade end users in real time and provide constructive feedback on:

- Active listening skills
- Empathetic validation of concerns
- Use of supportive statements
- Ability to restate and rephrase
- Provision of warm referrals
- Identification of need for further assistance (i.e., same-day mental health appointments, in-depth assessment, or additional screening).

Key Deliverables:

- Suicide prevention scenario scripts and user stories based on VA-approved language.
- Initial and updated VR prototypes for role-playing exercises.
- AI-enabled server software for dynamic responses and evaluation.
- User testing results and feedback synthesis reports.

3.2.3 PHASE 2: Field Test/Pilot

Phase 2, additional 12 months, will focus on field testing of updated solution based on Phase 1 product iteration following user testing and feedback. This will include Contractor travel to select VA sites to complete field testing and feedback capturing in-person. Field testing will also lead to iterative refinement of the solution after feedback received from each participating site. Phase 2 shall culminate in a product ready for operational capability within the VA and contractor shall transfer all necessary files and resources to allow VA to take ownership of the product for iterative development post-contract.

Key Deliverables:

- Updated backlog with features required for field testing.
- Release candidate build to start field testing.
- Field testing results and feedback synthesis reports.
- Provision of final prototype of the application, suitable for scaling, to VA for ownership

3.3 INTENDED BENEFITS OF THE SOLUTION

By adapting established curricula to a VR platform, Contractor shall create an immersive and interactive learning experience that enhances the effectiveness of suicide awareness training. This approach allows medical staff to practice critical skills in a safe, controlled environment, improving their ability to identify and respond to potential suicide risks. The VR format enables participants to engage with realistic scenarios, fostering deeper understanding and retention of key concepts while providing opportunities for immediate feedback and skill refinement. The interactive nature of VR

allows trainees to develop crucial empathy and communication skills through one-on-one role-playing exercises. This approach enhances engagement and retention, enabling staff to better understand the complexities of identifying suicide risks. This solution intends to complement existing educational tools by offering a unique, experiential learning opportunity that builds confidence and competence in this critical priority area of healthcare. By implementing VR training for management of suicide risk, the VA can equip a wider range of staff with the skills and confidence needed to intervene early. This proactive approach has the potential to significantly impact suicide prevention efforts among the Veteran population while also being adaptable to other modalities (e.g., telehealth.).

Key intended benefits include:

Benefit	Description
Enhanced Realism	<ul style="list-style-type: none"> • VR simulations can replicate nuances like body language, tone, and environments. • VR training enables role-playing scenarios for special populations at VA.
Reduced Anxiety and Increased Engagement	<ul style="list-style-type: none"> • VR environments offer a low-stakes practice space, reducing trainee anxiety. • Increased comfort leads to higher engagement and broader range of approach strategies.
Consistency and Scalability	<ul style="list-style-type: none"> • Standardized, replicable VR scenarios ensure consistent training quality. • VR provides a scalable solution ideal for large organizations like the VA.
Immediate Feedback and Iterative Learning	<ul style="list-style-type: none"> • AI systems provide instant performance feedback, offering immediate correction and improvement opportunities. • Repeatable scenarios with variations reinforce learning and adaptation.
Cost-Effectiveness	<ul style="list-style-type: none"> • Reduces expenses for in-person trainers, travel, and physical spaces. • VR headsets cost less than single overnight training trips

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) is one 12-month Base Year with Optional Tasks.

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

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

Under current definitions, five 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

Some tasks under this PWS shall be performed in VA facilities located at:

Atlanta VA Medical Center
1670 Clairmont Rd.
Decatur, GA 30033

Western North Carolina VA Healthcare System
1100 Tunnel Rd.
Asheville, NC 28805

Richmond VA Medical Center
1201 Broad Rock Blvd.
Richmond, VA 23249

Additional VA Facilities to be engaged pre- and post award utilizing existing VA networks. Work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR).

Additional tasks under this PWS, other than user and field testing site visits, shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their proposal and as stated below:

Customer Value Partners, LLC
805 Fifteenth St, Suite 650
Washington, D.C. 20005

4.3 TRAVEL

All travel requirements (including plans, agenda, itinerary, and dates) shall be pre-approved by the COR (subject to local policy procedures) at a minimum of seven (7) days prior to the trip, unless otherwise coordinated with the COR, and is strictly on a cost reimbursable basis, in accordance with Federal Travel Regulations (FTR). See FAR 31.205-46 Travel Costs. Trip Reports shall be submitted to the COR within five business days after trip completion. Each contractor invoice shall include copies of ALL receipts that support the travel costs claimed in the invoice. General and Administrative expenses will not be reimbursed.

The Government anticipates travel under this effort to perform associated tasks, throughout the PoP. Include all travel costs in your firm-fixed price line items. These costs will be directly reimbursed by the Government.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 TECHNICAL KICKOFF MEETING

The Contractor shall hold a project kickoff meeting within ten days after contract award. This meeting should be held via teleconference and/or web meeting. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each specific task and deliverable. The Contractor shall specify date, virtual meeting information, agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes shall be provided to all attendees within three calendar days after the meeting. The Contractor shall invite the CO, Contract Specialist (CS), COR, VA Project Manager (PM), and any other attendees deemed necessary by the aforementioned VA personnel.

Deliverable:

- A. Project Kickoff Meeting Agenda
- B. Project Kickoff Meeting Minutes

5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall be in electronic form in Microsoft Word and Excel or Project formats. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

The plan should include detailed tasks and deliverables with specified duration, objective, approach, potential challenges and mitigation, plan for measuring

success or outcomes, completion criteria, deliverables, and responsible organization.

Deliverable:

A. Contractor Project Management Plan

5.1.3 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Excel or Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month.

The Monthly Progress Reports shall cover all work cumulatively completed during prior reporting periods, the current reporting period, and work planned for the subsequent reporting period, to include a summary of the progress made, project milestone schedule, challenges, successes, proposed changes, and next steps. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables, as applicable, and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall attend an up to weekly teleconference meeting, cadence to be determined by the VA Program Manager, to be held at a time convenient for both the government and the Contractor. The Contractor shall provide Teleconference Progress Meeting Minutes within two business days after the teleconference meeting. The Contractor shall provide weekly emails with the progress, issues, and mitigations to the VA Program Manager and additional VA team members as designated by the VA PM. This team will be introduced in the kickoff meeting.

Deliverable:

- A. Cumulative Monthly Progress Report
- B. Teleconference Progress Meeting Minutes
- C. Email Weekly to VA PM

5.2 PHASE 1 PROTOTYPING

5.2.1 PROTOTYPE SCENARIO DESIGN

Contractor shall, in collaboration with VA Program Manager and identified VA Subject Matter Experts (SMEs), review existing VA-approved language, suicide prevention training materials and curriculum. Contractor shall conduct meetings

with identified VA SMEs and other stakeholders to understand requirements and current VA approaches for training and then, based on information gathered, develop scenario outlines and scripts focused on suicide prevention, leveraging existing VA resources as approved by VA. Contractor shall provide those scripts to the VA PM and other SMEs for review and approval.

Contractor shall then create user stories based on those approved scripts and any applicable VA guidelines and will submit those to VA PM for review and approval.

Deliverables:

- A. Initial Scenario Outlines and Scripting
- B. Prototype User Stories

5.2.2 INITIAL PROTOTYPE DEVELOPMENT

Using approved prototype user stories and associated scripting, Contractor shall develop the initial basic VR prototype for role-playing exercises. This shall include implementation of core functionality and basic user interface in a VR environment and a 2-D interface. Development shall include only VA-approved language and approaches into the VR scenarios.

Deliverables:

- A. Basic VR Prototype for Role-Playing Exercises

5.2.3 DEVELOPMENT OF AI GRADING FUNCTIONALITY

The contractor shall develop, following VA policies and guidelines, an AI-enabled software system to embed in the solution to enable real-time evaluation of end-user responses to scenarios developed compared to the VA curriculum and best practices. This functionality shall be added to existing VR prototype for review by VA PM and SMEs for user testing.

Deliverables:

- A. AI Grading Prototype Functionality

5.2.4 SUSTAINABLE DATA ACCESS AND ANALYSIS

Contractor shall coordinate with VA Program Manager to determine metrics associated with project goals and specify the means of capturing required information in a data collection and analytics plan. Data collection and analytics plan will also include co-development of pre- and post-testing survey questions.

Contractor shall provide aggregated, deidentified data showing impact of solution including both quantitative and qualitative metrics as well as develop a means of

completing and visualizing data analytics accessible by VA. Contractor shall use the REAIM evaluation framework to evaluate impact, value, and all associated processes and outcomes, in all phases of this project. Final plan for data collection and analysis, including metrics, shall be presented to the VA Program Manager for approval before developing a data analytics visualization solution. The Contractor shall develop a means of accessing data metrics and analytics determined and approved by VA PM that will be accessible to VA. Once Contractor has developed a resource for providing real-time data analytics visualization, VA PM must be provided access for review and approval. Resource may be tested and iterated upon in Phase 1 and Phase 2.

Deliverables:

- A. Data Collection and Analysis Plan
- B. Project Data Access Resource with Real-time Data Analytics Visualization

5.2.5 PHASE 1 USER TESTING AND PRODUCT ITERATION

Prior to beginning user testing, Contractor shall develop a Phase 1 User Testing Plan and provide to the VA PM for review and approval. Then, to enable participation from site-level providers and other subject matter experts, Contractor shall develop and coordinate the signing of memorandums of understanding (MOUs) between participating sites, the Office of Healthcare Innovation and Learning, and the Office of Suicide Prevention. Phase 1 User Testing shall be conducted with a minimum of 3-5 sites, 10 users at each site.

Contractor shall conduct initial user testing with VA SMEs and other VA-designated site-based participants. Contractor shall gather feedback on VR experience, content accuracy, and effectiveness of AI grading functionality using the agreed upon Data Collection and Analysis Plan. Once a user testing session(s) is complete, Contractor shall analyze and synthesize feedback, provide the results to the VA PM as a User Testing Feedback Report, including plans for iteratively refining content and approach prior to next User Testing session.

Contractor will then update user stories and create a Refined Product Backlog based on feedback received and will develop updated VR and 2D prototypes with that feedback to create a Final Prototype ready for additional User Testing and initial Field Testing in Phase 2.

Deliverables:

- A. Phase 1 User Testing Plan
- B. MOU Coordination for at least 5 Sites

Commented (b)(6); (b)(5)
(b)(5)
Commented (b)(6); (b)(5)
(b)(5)
Commented (b)(6); (b)(5)
(b)(5)

C. Phase 1 User Testing Feedback Report (5)

5.2.6 FINAL PHASE 1 REPORT

At the completion of Phase 1, Contractor shall provide to the VA Program Manager a Phase Summary Report, inclusive of all work completed during Phase 1 and all data analytics required to meet project goals and determination of innovation value.

Deliverables:

- A. Final Phase 1 Summary Report

5.3 OPTIONAL TASK – PHASE 2 FIELD TESTING

If VA exercises the Optional Task, the Contractor shall perform tasks identified in Sections 5.1 and all subsections, except 5.1.1. The period of performance for this optional task is 12 months. In reference to the deliverables in these sections, if the task has generated a document during the base period, the Contractor shall provide updates only. If VA exercises the Optional Task, the Contractor shall also perform the following:

5.3.1 FIELD TESTING AND PRODUCT ITERATION

Prior to beginning field testing, Contractor shall develop a Phase 2 Field Testing Plan, including all pre-determined metrics and evaluation criteria from the Data Collection and Analysis Plan, and provide to the VA PM for review and approval. Field testing shall include a collection of data pre-testing, immediately following testing, and at 8 weeks post-testing. To enable participation from site-level providers and other subject matter experts, Contractor shall develop and coordinate the signing of memorandums of understanding (MOUs) between additional participating sites, the Office of Healthcare Innovation and Learning, and the Office of Suicide Prevention. Phase 2 Field Testing evaluation shall be conducted with a minimum of 5-10 sites, minimum 10-20 participants at each site, in a configuration that ensures at least 100 total participants in Phase 2. 5-10 individuals at each site will participate in VR training with pre-determined pre- and post-questions, and 5-10 will only complete existing training but will complete the same pre- and post-questions, with a goal of having 50 participants in the VR group and 50 in the control group. Contractor shall coordinate dates for on-site visits to each participating site, prepare for and travel to sites, setup equipment for multiple testing sessions, instruct users how to use the solution (if in VR group), document all feedback, and facilitate completion of pre-questions and immediate post-questions with all participants at site. Contractor will then follow-up with participants 8 weeks later to request completion of additional post-questions. Contractor shall provide 5 VR headsets to each participating site that the site will retain ownership of following field testing completion.

Commented (b)(6) 1: (b)(5)
(b)(5)
Commented (b)(7) 8: (b)(5)
(b)(5)
Commented (b)(6) 8: (b)(5)
(b)(5)
Commented (b)(6) 2: (b)(5)
(b)(5)
Commented (b)(6) 12: (b)(5)

Once a field testing site visit is complete, Contractor shall aggregate quantitative and qualitative feedback and data from the field site and provide the results to the VA PM as a Field Testing Report, including plans for iteratively refining content and approach prior to next Field Testing site visit.

Contractor will update VR and 2D solutions using Field Testing feedback, if changes approved by VA PM, to create a final product ready for operationalizing. This may include updating user stories, imagery, functionalities, or any necessary and feasible changes to ensure a satisfactory product. Application shall be converted from prototype status to one ready for initial operational capability. Contractor shall create “how to” guides and any resources required by VA prior to performance period completion. Contractor shall enable the auto-update feature so headsets can be updated remotely while in the field. All files and resources to allow VA to continue iteration and further development of the solution post-performance period shall be provide to the VA PM prior to contract expiration – transferring ownership of the solution to the VA.

Deliverables:

- A. Phase 2 Field Testing Plan
- B. MOU Coordination for at least 10 Sites
- C. Phase 2 Field Testing Report (10)
- D. Final Product, both VR and 2D versions, including necessary APK files/source code

5.3.2 OPERATIONAL PLAYBOOK FOR SUSTAINABILITY AND SCALABILITY

Based on results of all User and Field testing, and with any additional feedback and insights from VA participants and SMEs, Contractor shall develop a uniform process via an Operational Playbook for Sustainability and Scalability for implementing the solution with additional sites in the future and plan for integration of solution with VA’s Talent Management System in a manner to allow tracking of training completion.

Deliverable:

- A. Operational Playbook for Sustainability and Scalability

5.3.3 PHASE 1 AND PHASE 2 COMBINED FINAL REPORT

At the completion of Phase 2, Contractor shall provide to the VA Program Manager a Project Summary Report, inclusive of all work completed during Phase 1 and 2 and all data analytics (initial data analyses and final data analyses of all data captured during all periods of performance) required to meet project goals and determination of innovation value. Summary Report will also include

detailing the process and outcomes, including recommendations for additional testing, scalability, and/or integration with other VA Resources.

Deliverable:

- A. Phase 1 and Phase 2 Final Project Report

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

Not Applicable

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	x <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	x <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	x <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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. 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 PAL template artifact. 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.

- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
- d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed SIC Fingerprint Request Form
- e. 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).
- f. 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 e-QIP).
- g. 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.
- h. 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), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. 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 OPM.

- i. 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.
- j. 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.
- k. 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 Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none"> 1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none"> 1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems 	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none"> 1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks 	Satisfactory or higher
D. Management	<ol style="list-style-type: none"> 1. Integration and coordination of all activities to execute effort 	Satisfactory or higher

The COR 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 level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.5 FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will 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.

6.6 GOVERNMENT FURNISHED PROPERTY

Not Applicable

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, unless the connection uses FIPS 140-2 (or its successor) validated encryption, 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: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about->

[the-section-508-standards/section-508-standards](#). 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 Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment.

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 of 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.

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

B1. GENERAL

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

NOTE: Any sections (1-14) which DO NOT apply should not be included in the Statement of Work (SOW), Performance Work Statement (PWS), Product Description (PD) or contract.

B2. VA INFORMATION CUSTODIAL LANGUAGE

This entire section applies to all acquisitions requiring any Information Security and Privacy language.

- a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*. The primary clause used to define computer software license (not data/intellectual property first produced under this contract or order) is FAR 52.227-19, *Commercial Computer Software License*.
- b. Information made available to the contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*.
- c. VA information will not be co-mingled with any other data on the contractor's information systems or media storage systems. The contractor shall ensure compliance with Federal and VA requirements related to data protection,

data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

- d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to contractor and subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.
- e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.
- f. The contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.
- g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.
- h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.
- i. The contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.
- j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA

information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.

- k. Notwithstanding the provision above, the contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality- assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the contractor is in receipt of a court order or other requests for the above- mentioned information, the contractor shall immediately refer such court order or other requests to the VA CO for response.
- l. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.
- m. Any data destruction done on behalf of VA by a contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.
- n. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, *Guidelines for Media Sanitization* prior to termination or completion of this contract. If directed by the COR/CO, the contractor shall return all Federal Records to VA for disposition.
- o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.
- p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to

the contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

q.

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS.

This section

applies when any person requires access to information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract.

- a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of contractor/subcontractor and agent of contractor/subcontractor.
- b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.
- c. All contractors and subcontractors working with VA information are subject to the same security investigative and clearance requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).
- d. All contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All contractors and subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United

States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the contractor must state where all non-U.S. services are provided. The contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

- e. The contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
 - 1. Contractor/subcontractor personnel no longer has a need for access to VA information or VA information systems.
 - 2. Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.
 - 3. Contractor believes their own personnel or subcontractor personnel may pose a threat to their company's working environment or to any company- owned property. This includes contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.
 - 4. Any previously undisclosed changes to contractor/subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.
 - 5. Contractor/subcontractor personnel have their authorization to work in the United States revoked.
 - 6. Agreement by which contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for contractor personnel.
- f. In such cases of contract fulfillment, termination, or other causes; the contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by contractor/subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.
- g. Contractors/subcontractors who no longer require VA accesses will return VA- issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems,

networks and VA property in their possessions removed, contractors shall notify the appropriate VA COR/CO.

B4. TRAINING.

This entire section applies to all acquisitions which include section 3.

- a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:
 1. VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.
 2. Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and
 3. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role- based information security training].
- b. The contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.

B5. SECURITY INCIDENT INVESTIGATION.

This entire section applies to all acquisitions requiring any Information Security and Privacy language.

- a. The contractor, subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the contractor, subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.
- b. To the extent known by the contractor/subcontractor, the contractor/ subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:
 - 6 The date and time (or approximation of) the Security Incident occurred.

- 6 The names of individuals involved (when applicable).
 - 6 The physical and logical (if applicable) location of the incident.
 - 6 Why the Security Incident took place (i.e., catalyst for the failure).
 - 6 The amount of data belonging to VA believed to have been compromised.
 - 6 The remediation measures the contractor is taking to ensure no future incidents of a similar nature.
- b. After the contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The contractor, subcontractor, and their employees 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.
 - c. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.
 - 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 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.
 - e. The contractor shall comply with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.
 - f. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.
 - g. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated

damages to the VA as set forth in clause [852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs](#).

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT.

This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (to include the subcomponents of each) designed or developed for or on behalf of VA by any non-VA entity.

- a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).
- b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.
- c. VA IT contractors, subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, *Risk Management Framework for Cloud Computing Services* and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work through the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.
- d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M- 22-18 (September 14, 2022). The term "software" includes firmware, operating systems, applications and application services

(e.g., cloud-based software), as well as products containing software. The contractor shall provide a self- attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self- attestation.

- e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.
- f. The contractor shall ensure all contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.
- g. The contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository.
- h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default "program files" directory with silently install and uninstall. The contractor shall