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	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	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.Staffing	1.Currency of expertise and staffing levels appropriate 2.Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D.Management	1.Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR shall 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

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

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

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 shall have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.

3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

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 R*ights 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 contactor.

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

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

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

k. Notwithstanding the provision above, the contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality- assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia,

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

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

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

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

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

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

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS.

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:
    1 The date and time (or approximation of) the Security Incident occurred.
    2 The names of individuals involved (when applicable).
    3 The physical and logical (if applicable) location of the incident.
    4 Why the Security Incident took place (i.e., catalyst for the failure).
    5 The amount of data belonging to VA believed to have been compromised.
    6 The remediation measures the contractor is taking to ensure no future incidents of a similar nature.

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 employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

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

m. 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.

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

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE.

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.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).
e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with contractor activities are also subject to such assessments. The contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.
f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.
g. The contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using Government personnel or a third-party if deemed necessary. The contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required

for Government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved contractor OE will be subject to technical inspection at any time.

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

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

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

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

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.

B9. 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.

B10. 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:
    1. Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware

throughout VA's information networks, computer systems and information systems; and

2. Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

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.

B12. 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:

    1. The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and
    2. The approach and capability to remediate newly reported zero-day vulnerabilities for contractor products.

b. The contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.
c. The contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by contractor within these time periods, the contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.
d. The contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third- party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

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

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 though the COR/CO for governance or resolution.

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

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

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

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

g. The contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.
h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive. information will be returned to the contractor with media removed. When the contract requires return of equipment, the options available to the contractor are the following:
    1. The contractor shall accept the system without the drive, firmware and solid state.
    2. VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn- in; or
    3. Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:
        a) The equipment contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.
        b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

B14. DATA CENTER PROVISIONS. 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.

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

VARA Smart Safe & App for Secure Firearm Storage And Veteran Suicide Prevention

1.0 BACKGROUND

As an innovation engine within the Department of Veterans Affairs, the vision of the Veterans Health Administration's Innovation Ecosystem (VHAIE) within the Office of Healthcare Innovation and Learning 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 through fostering organizational capability, delivery of operational and clinical breakthroughs, and by 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.

Commented (b)(5)

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.

We therefore begin 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, 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.aspNIST 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

3.0 SCOPE OF WORK

This contract and proposed solution focus on the following topic:

- Promote secure firearm storage for Veteran suicide prevention.

Topic Detail: Promote secure firearm storage for Veteran suicide prevention. Firearm ownership and storage practices vary among Veterans. One in 3 Veteran firearm owners store at least 1 firearm unlocked and loaded. This unsafe storage practice is more frequent among Veteran firearm owners who seek VHA care (38.0%) than among other Veterans who own firearms (31.9%).36 As seen across years of Veteran suicide data, Veteran suicide deaths disproportionately involve firearms; Veteran suicide rates exceed those of non-Veterans; and differentials in suicide rates by Veteran status are greater for women than for men. Promoting secure storage of firearms has been found to reduce suicide — this is not about taking away firearms but about promoting time and space during a time of crisis.

References for initiatives related to Mann JJ, Michel CA, Auerbach RP. 2021. Improving Suicide Prevention Through Evidence-Based Strategies: A Systematic Review. American Journal of Psychiatry. 178(7):611-624

3.1 Specific Problem to Address with this Solution:

Government funding and safe storage initiatives have accomplished the widespread distribution of the gun cable lock. However, unsecured firearms are still a prominent issue in Veteran suicide prevention and alternative storage options are needed. A recent study on secure firearm storage behavior indicated that solutions such as lock boxes are preferred when it comes to firearm storage and more likely to be used. Being

able to effectively quantify and track the metric of usage is also an unmet need in suicide prevention.

Vara is focusing on three critical unmet needs in suicide prevention:

1. Despite widespread distribution of cable locks, many Veterans still choose not to utilize a secure storage device. What can be done to improve usage?
2. After distribution of a secure storage device, researchers are finding it difficult to quantify the success of the program in terms of actual use. How could better data be collected?
3. More innovation. What solutions would Veterans really use to delay access?

Here are the critical problem areas that we discovered from gun-owning Veterans:

1. Veterans have a strong desire for fast access to their firearms. This is driven by their need to quickly get to a firearm in an emergency and protect themselves.
2. Veterans have a fear that their firearms may be taken away if they talk about their mental health problems or seek help.
3. Veterans care about their data privacy, especially in regards to what information the government has about their ownership of firearms.
4. Veterans have a higher threshold of comfort with keeping an unsecured, loaded firearm, especially for those who lived under such circumstances during deployment. Therefore, unsecured firearms are a lower perceived risk.

3.2 Proposed Solution:

Promote firearm secure storage by adding movement detection in real time alerts to a firearm lock.

The Vara Smart Safe is a compact, secure, digital lock box. This lock box will operate with a keypad and the user can set a unique passcode to unlock the device. It will be battery operated and will last up to one year on a single charge. It includes "smart" electronics that enable the lockbox to connect with an app through WiFi.

The Vara Smart App (or "App") is a digital application designed for Veteran suicide prevention. It connects with the Smart Safe and consists of four main features:

1. Lock Out Mode
2. Two Factor Mode
3. VA Resources
4. Data Analytics Platform

3.2.1 Project Metrics

Contractor shall collaborate with VA Program Manager on project metric determinations aligned with the REAIM evaluation framework for all phases of this project. VA PM must approve metrics prior to beginning user testing. The contractor shall detail the testing strategy, agreed-upon metrics and method of tracking, and proposed timeline in the Evaluation Plan and must be approved by VA Program Manager.

3.2.2 PHASE 1

The first phase shall use a mixed methods design with qualitative focus groups and brief qualitative focus groups and brief quantitative surveys administered at the beginning of each focus group. Focus group protocols will address key questions outlined above. Brief surveys will collect demographics and assess participants' familiarity and proficiency with smart apps. Vara's development team will ensure key user feedback is collected.

The first phase of the evaluation shall solicit veteran firearm owners' in-depth feedback about usability and acceptability of the Vara Smart Safe and App. This qualitative and quantitative data from the focus groups and surveys will also be shared with the VA via a progress report during the testing and a final report at the end of Phase 1.

Participants will be recruited from among Veterans who own firearms, with efforts to include a ranges, of Veterans from across the US. In addition to Vara's network of email subscribers and social media followers, focus group participants will have the option to participate in the subsequent longitudinal study. Rapid qualitative analysis will be conducted after each focus group data collection effort. Survey responses shall be summarized descriptively.

After each round of focus groups and surveys, findings will be synthesized into a written summary with recommendations that is shared with Vara to inform their revisions and finalization of the lockbox and Smart App.

During the Prototype/Test Phase, the Vara engineering team will be responsible for completing the final technical development of the Vara Smart Safe and App.

3.2.3 PHASE 2

To address key questions for Veterans, this phase shall use a mixed methods longitudinal design with repeated data collection among participants who own firearms, receive the lockbox, and have downloaded the suicide prevention Smart App. First, participants shall complete a baseline survey of self-efficacy as a measure of perceived control and a survey to assess familiarity, experience, and proficiency with smartphones and digital apps.

The research team will engage with participants to conduct semi-structured interviews and surveys about usability and acceptability of the Smart Safe and Smart App features, perceived benefits and drawbacks, intentions, norms, and their beliefs about secure firearm storage and about the lockbox and Smart App as a suicide prevention tool. In addition, the research team will receive de-identified quantitative usage metrics from Vara reflecting participants' use of the suicide prevention app features. Usage metrics may include Smart Safe data and app feature access data.

Deliverables shall include a two-page summary shared with Vara to discuss implications of the evaluation on product development and dissemination; dissemination at a relevant conference, if appropriate; and development of one or more manuscripts for peer-reviewed publication.

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 10 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

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:

687 Rowley Road
PO BOX 355
Victor, New York 14564

4.3 TRAVEL

The Government anticipates travel under this effort to perform associated tasks, throughout the period of performance. Include all travel costs in your firm-fixed price line items.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

The contractor shall pursue any technical requirements for establishing consent for data sharing for pilot participants and data use agreements and arrangements between stakeholders required for development and evaluation of the prototype.

This shall include any Institutional Review Board (IRB) requirements as determined by the vendor and the government. The contractor shall establish closed and secure data security environments as required by stakeholders and all applicable data use agreements between parties.

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 deem 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.

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 completed during the 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 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 up to weekly teleconference meeting, cadence to be determined by 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 the VA PM

5.2 Prototyping & Test Phase (Base Period)

5.2.1 Veteran Centered Design Study

The Contractor shall engage with a group of at least 60 Veterans from across the United States that is representative of military service persons. The Contractor shall create any needed surveys, interview instruments, and focus groups, in collaboration with the VA PM. Contractor shall deliver a summary report of findings synthesized into a written summary to inform revision and finalizations of the lockbox and Smart App.

Deliverable:

A. Veteran Centered Design Summary Report

5.2.2 Recruitment Strategy Planning

The Contractor shall deliver a pilot recruiting strategy to be implemented in Phase 2. The recruiting strategy, in order to determine whether the prototype is feasible and acceptable among gun owners, shall be designed for and include Veterans as described in section 5.2.1. The purpose for these types of Veterans is to evaluate user engagement differences among these different Veteran subgroups.

Deliverable:

A. Draft Recruitment Strategy
B. Final Recruitment Strategy

5.2.3 Evaluation Planning

The contractor shall deliver an evaluation plan to be implemented in Phase 2 with the REAIM framework. The contractor shall research, discover, and elicit the the specific criteria to be evaluated in order to determine the feasibility and acceptability of the prototype Smart Safe and associated app.

Deliverable

A. Draft Evaluation Plan for Pilot
B. Final Evaluation Plan for Pilot

5.2.4 Prototype Development and Delivery

The contractor during the first phase shall further refine the technology, customization, and veteran/family/friend focused input to allow for the best design of a working prototype and alert system by the end of the base period. The contractor shall provide an in-person or virtual demonstration, as determined by the COR or VA program manager, of the prototype. Prototype shall be delivered to a location as determined by the COR or VA program manager.

The contractor shall create a testing plan for technology and provide any corrective actions if needed. They shall also accomplish any testing for hardware review and provide for corrective action as needed.

Deliverables:
A. Prototype Demonstration
B. Phase 1 Prototype

5.2.5 Phase 1 Final Report and Evaluation

The Contractor shall provide complete reporting of findings and recommendations for the Phase 1 Final Report prior to the end of Phase 1 for review by VA stakeholders and business owners. This report should include a detailed inventory of all iterative changes made or planned to be made based on feedback and data collected.

The Contractor shall also provide a Final Phase 1 Report of results from the tasks performed in Phase 1 to include challenges, successes, proposed or completed changes, PWS progress, next steps recommending updates for implementation plan for the Pilot Study, in the Option Period, if exercised by VA. The contractor shall deliver a final Pilot Design Briefing with the Phase 1 Final Report

Deliverables:
A. Phase 1 Final Report
B. Pilot Design Final Briefing

5.3 OPTIONAL TASK

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 Phase 2 Field Testing

The contractor shall recruit at least 500 participants for field testing of the tailored prototype and deploy any surveys required during Phase 2. The contractor shall conduct any qualitative interviews that are needed to evaluate user experience and engagement.

Contractor shall provide for the shipping and delivery of product to study participants. Contractor shall provide any technical assistance and customer service required to study participants.

Contractor shall provide a field summary report of Phase 2 testing data as directed by VA program manager.

Deliverables:
A. Phase 2 Field Summary Report

5.3.2 Final Prototypes

The contractor during the second phase shall further refine the technology, customization, and veteran/family/friend focused input to allow for the best design of a tailored prototype and alert

system by the end of the optional period. The contractor shall provide an in-person or virtual demonstration, as determined by the COR or VA program manager, of the prototype. Prototypes, up to five, shall be delivered to a location as determined by the COR or VA program manager.

The contractor shall create a refinement testing plan for technology and provide any corrective actions if needed. They shall also accomplish any testing for hardware review and provide for corrective action as needed.

Deliverables:
A. Final Prototypes (5)

5.3.3 Phase 2 Evaluation and Final Report

The Contractor shall provide a Pilot Implementation Final Project Report and Summary to include project findings, summary of recommendations to VA for next steps, which could include additional testing, scalability, and/or integration with other VA resources.

Deliverable:
A. Initial Findings Report
B. Final Project Findings and Summary 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☒	☐	☐
5.2	x☒	☐	☐
5.3	x☒	☐	☐

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	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	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	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	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 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 AND PRIVACY LANGUAGE FOR INCLUSION IN CONTRACTS, AS APPROPRIATE

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.

1. **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.
2. **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 R*ights 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 contactor.

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.

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.
   (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.

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:
      - VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.
      - 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
      - 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:
      1. The date and time (or approximation of) the Security Incident occurred.
      2. The names of individuals involved (when applicable).
      3. The physical and logical (if applicable) location of the incident.
      4. Why the Security Incident took place (i.e., catalyst for the failure).
      5. The amount of data belonging to VA believed to have been compromised.

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

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

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 though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.
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 of1974 (the Act), FAR 52.224- 2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

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

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 though the COR/CO for governance or resolution.
c. The contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.
d. The contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Postmarket Management of Cybersecurity in Medical Devices.

e. The contractor shall design devices capable of accepting all applicable security patches with or without the support of the contractor personnel. If patching can only be completed by the contractor, the contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.
f. The contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the contractor cannot install an anti-virus / anti-malware application.
g. The contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.
h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the contractor with media removed. When the contract requires return of equipment, the options available to the contractor are the following:

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

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.

B.4 PERFORMANCE WORK STATEMENT

-

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Veterans Health Administration (VHA)
VHA Innovation Ecosystem (14HIL1)

Anonymous Peer Groups

Date: 25 November 2024
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 the VA to source incremental and transformational innovations to best serve Veterans and their families.

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.

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," 2014
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.aspNIST 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

3.0 SCOPE OF WORK

This contract and proposed solution focus on the following topic:

- **Implement and sustain community collaborations focused upon community-specific Veteran suicide prevention plans**

Topic Detail: Implement and sustain community collaborations focused upon community-specific Veteran suicide prevention plans. Over 60% of Veterans who died by suicide in 2021 were not seen in VHA in 2020 or 2021, and over 50% had received neither VHA nor VBA services. In order to reach all Veterans, we must continue to expand our work in the community through the SP 2.0 Community Based Intervention (CBI) Program. This includes the joint VA and Substance Abuse and Mental Health Services Administration (SAMHSA) Governor's Challenge to Prevent Suicide Among Service members, Veterans, and their Families, which encompasses all 50 states, 5 territories and work in over 1,700 local community coalitions. This also includes the SSG Fox SPGP awarding $52.5 million to 80 community-based organizations in 43 states, the District of Columbia and American Samoa in fiscal year (FY) 2023.

Specific Problem to Address with this Solution.

Barriers to VA mental health care access are multifold and may include stigma (fear of what others will think or fear for career impact, trust, or privacy issues), logistical (cost, transportation), and eligibility limitations. Solutions are needed to address those barriers through both community and VHA-accessed resources.

Proposed Solution.

Cabana provides confidential, professionally moderated peer support groups and psychoeducational content, through self-guided micro learning and personalized learning journeys, intended to break stigma and encourage early intervention for Veterans not currently engaged with VA care. The proposed solution leverages community-based partnerships with SSG Fox SPGP community hubs to extend support into trusted, non-VA environments.

The Contractor shall provide enhancements and Subject Matter Expertise (SME) to the existing Cabana system (Apple IOS). The Contractor shall develop a production ready version of the Cabana system for the Android operating system. The Cabana system (Apple IOS) is currently available from the Apple Library. The contractor shall offer the production ready version for Android on the Google Play Library once available. The contractor shall perform usability testing and feasibility testing (online mobile application, with a clinical user dashboard, and adjunct subclinical mental health virtual resource) with each operating system, Apple IOS and Android. Testing shall be completed in a two-phase approach. The REAIM framework will be used to evaluate impact in both phases. Reasons for non-adoption shall be identified, and a resolution/mitigation process will be created and adopted.

Phase 1 (first 6 months) to focus on building infrastructure, testing user experience, and optimizing platform for field testing deployment. Phase 2 (second 18 months) to focus on development of Android version and testing feasibility, scalability, and effectiveness. Initiation of Phase 2 is dependent on satisfactory performance in Phase 1.

The contractor shall complete software testing including automated testing, requirements gathering and analysis, user/stakeholder research, project management, technical writing, develop training material and application demonstrations.

3.1 PHASE 1

Phase 1 will be completed with two identified VA medical centers and two Veteran Service Organizations (VSO) in the respective states of North and South Carolina. The primary intent of Phase 1 is platform user testing and custom prototyping. Feedback from Veterans and VA clinicians shall be used to make iterative changes and programmed into the current (IOS) version of the Cabana Platform. Phase 1 will also include establishing necessary operational partnerships, building technical infrastructure, and capturing and sharing data for all proposed metrics with VA team. All Veteran patients who participate will be screened through the VA Staff Sargent (SSG) Fox Suicide Prevention Grant Program community hubs. During Phase 1, the project team shall collaborate with partnering VA teams in VISN 6 and 7 along with their VSO partners, to complete beta testing of the Cabana Platform's elements (online (IOS) mobile applications, data sharing mechanism, and adjunct subclinical mental health

resource). A minimum of 50 Veterans will be enrolled in prototype and UX testing of the iOS version of the solution.

Phase 1 Metrics:

Reach	• Track number of Veterans enrolled and engaged with platform • Track number of intra-network referrals from community partners to solution. • Veteran demographics (age, sex, branch of service)
Effectiveness	• Time to support – measured by time from account creation to first live group attendance • Assess ability to reduce stigma and increase engagement through user feedback and participation rates • Mental Health Minutes (Time in Application) • Monthly and weekly user rate to monitor user activation and retention • Average group scores (rated 1-5) on technology, group quality, moderator performance
Adoption	• Track ease of use • Track referral engagement • Track enrolled Veterans • Platform utilization • Group session attendance • Participation frequency • Engagement with micro-learning modules and Voyage feature
Implementation	• Alignment with Veteran needs • Ease of deployment • Effectiveness of Hub to Cabana and Cabana to VA referrals minimizing admin burden on VA staff • UX improvements made based on feedback
Maintenance	• Success of operational integration • Impact of prototype deployments on field testing phase

3.2 PHASE 2

In Phase 2, an Android version of the Cabana platform shall be created in accordance with Google applications and be available on the Google Play Store for download. The contractor shall complete platform user testing and custom prototyping. Feedback from Veterans and VA clinicians shall be used to make iterative changes and programmed into the current (Android) version of the Cabana Platform. The processes and method of recruitment, enrolling veterans to use the Cabana platform, and eventual referral to formal Veteran Affairs Health services, shall be used with three additional Veteran Service Organizations and 3 additional VA medical centers to increase enrollment to a minimum of 1000 unique veterans. This expansion will further validate the feasibility,

effectiveness, and scalability of the Cabana Platform solution. This phase should include full field testing of both the Android and iOS versions of the Cabana platform, co-design and introduction of a mode of sustainable data analytics reporting to allow community partners and VA to jointly monitor aggregate utilization and referral data, enhancement of single sign-on capabilities and user interface, and include development of a long-term scaling and sustainability plan. Phase 2 will also include capturing and sharing data for all proposed metrics with VA project team.

Phase 2 Metrics:

Reach	• Track number of Veterans enrolled and engaged with platform across 5 hubs • Track number of intra-network referrals from community partners to solution. • Track number of referrals from Cabana to formal VA mental health services including occurrence and timing of VA services utilization alongside Cabana support • Track retention rates • Veteran demographics (age, sex, branch of service)
Effectiveness	• Time to support – measured by time from account creation to first live group attendance • Assess ability to reduce stigma and increase engagement through user feedback and participation rates • Mental Health Minutes (Time in Application) • Monthly and weekly user rate to monitor user activation and retention • Average group scores (rated 1-5) on technology, group quality, moderator performance • Outcome improvements
Adoption	• Uptake of resources across all hubs • Track ease of use • Track referral engagement • Track enrolled Veterans
Implementation	• Effectiveness of Hub to Cabana and Cabana to VA referrals minimizing admin burden on VA staff • UX improvements made based on feedback • Alignment with Veteran needs • Ease of deployment at new hubs • Feedback on ease of use • Feedback on referral system integration
Maintenance	• Success of operational integration • Impact of prototype deployments on field testing phase Sustainability in community and VA workflows

	• Development of long-term scaling and sustainability plan

3.3 INTENDED BENEFITS OF THE SOLUTION

The Cabana Platform program is designed to improve suicide prevention, awareness, engagement, and education in a manner that allows individuals to evaluate risk factor information and/or determine their risk for suicide or its progression in a virtual environment.

Solution implementation is intended to bridge the gap between community outreach or support and formal VA clinical care by providing initial access to support outside of VA for those Veterans not yet seeking or enrolled in VA mental health care or who may be ineligible for VA mental health care. Through the Cabana platform, the hope is at-risk Veterans receive timely, community-based support to augment VA's efforts to increase Veteran outreach, reduce stigma, normalize mental health support, provide access to digital health resources, and engage those Veterans not yet in VA care.

- Reduce Social Isolation
- Foster early engagement with at-risk Veterans
- Help prevent crises and reduce likelihood of suicide
- Removes geographical and logistical barriers to increase access to mental health support
- Augments VA suicide prevention and outreach efforts
- Potential for operational scalability due to group-based model and ability to integrate within existing community organizations
- Potential for cost efficiency to be impacted by reduced need for individual clinical appointments and virtual group model operating at a lower cost per Veteran.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) is one 6-month Base Period 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 10 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
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:

- VA Mid-Atlantic Health Care Network VISN 6
  3518 Westgate Drive
  Durham, NC 27707 Phone: 919-956-5541

- VA Southeast Network VISN 7
  3700 Crestwood Parkway Suite 500
  Duluth GA 30096 Phone: 678-924-5700

- VA Capital Health Care Network VISN 5
  849 International Drive, Suite 275
  Linthicum, MD 21090. Phone: 410-691-1131

- VA Healthcare VISN 4
  1010 Delafield Road
  Pittsburgh, PA 15215 Phone: 412-822-3316

Some Tasks under this PWS shall be performed in collaboration with Veteran Service Organizations:

- Upstate Warrior Solution (UWS)

- Veterans Bridge Home (VBH),

- Asheville Buncombe Community Christian Ministry, Inc.,

- Veteran Leadership Program (Western PA)

- Georgia Department of Veterans Services,

- EveryMind, Inc. (DC, MD, VA).

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:

- Even Health LLC (DBA "Cabana")
  209 West Street, Suite 202 Annapolis, MD 21401

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.

Local travel within a 50-mile radius of VA Central Office 810 Vermont Avenue, NW, Washington, D.C. 20420 is considered the cost of doing business and will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Travel beyond a 50-mile radius of VA Central Office 810 Vermont Avenue, NW, Washington, D.C. 20420 is authorized on a case-by-case basis and must be pre-approved by the COR a minimum of seven (7) days prior, unless coordinated with the COR.

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 deem 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 reports 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, if any, 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 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 Program Manager

5.2 Platform Testing and Evaluation

5.2.1 Collaboration Agreements and Onboarding of Veteran Service Organizations

The Contractor shall develop and execute formal partnerships with a minimum of 2 community hubs/Veteran Service Organizations. Collaborator shall work with those enrolling Veterans in the Staff Sargent (SSG) Fox Suicide Prevention Grant Program at each of the identified VSOs and with their corollary VHA referral intake personnel. Contractor shall establish Memorandums of Understanding (MOU) with all collaborating VSOs, and other supporting organizations as needed, including external organizations supporting evaluation, and provide a report on those established partnerships.

Formal partnership shall include the Contractor onboarding the community hub staff to promote familiarity and ensure smooth adoption of the platform. Contractor shall conduct joint quarterly review sessions with Community Hubs and VA PM, and additional VA team members as designated, to monitor progress and document lessons learned. Contractor shall provide to VA meeting minutes from those quarterly all-party review sessions.

Deliverable:

A. MOU Report
B. Quarterly All-Party Review Session Minutes

5.2.2 Recruitment Strategy

Contractor shall develop recruitment strategy, in collaboration with community hubs and VA PM and designated VA team members, to integrate Cabana into SSG Fox SPGP marketing and outreach activities at initial two community hubs. Contractor shall provide to the VA PM a Recruitment Strategy Plan for approval.

Contractor shall also collaborate with community hubs and VA to develop business processes and workflows for intra-network referrals, sign-ups, and crisis handoffs. Contractor shall provide to the VA PM a Referral and Enrollment Plan for approval.

Deliverable:

A. Recruitment Strategy Plan
B. Referral and Enrollment Plan

5.2.3 Platform Access and Usability Testing Plan

The Contractor shall provide access to a digital library of on-demand, therapist-curated psychoeducation tools, and resources for self-guided microlearning (available twenty-four hours a day, seven days a week (24/7)), Cabana's Personalized Learning Journeys

tailorable to individual users, and online live, professionally moderated peer support group sessions through the publicly downloadable Apple (IOS) version, for those with that type of personal device, of the Cabana mobile application to all participants in this pilot, Veteran patients, VSO stakeholders, Veterans Health Administration (VHÀ) Program, project staff and the acquisition contract support staff Contracting Officer's Representative (COR). The contractor shall maintain the software to include fixing defects, improving capabilities, and related functionality in support of the user community and VA, in addition to developing any needing training materials. Access in Phase 1 will be primarily focused on prototyping and usability testing, and a minimum of 50 Veterans will be enrolled in this phase. Access to the Cabana (iOS) platform shall be through the Apple Store and access for all parties above shall be confirmed by the Contractor and shared with VA through an Access Tracker as agreed upon by the VA Program Manager, including the minimum number of Veterans enrolled.

Contractor shall collaborate with VA PM in project metric determinations aligned with the REAIM evaluation framework for all phases of this project. VA PM must approve metrics prior to beginning user testing. The Contractor shall articulate the specific plan for usability testing of the Cabana (IOS) and the to-be-developed Android Platform with both Veterans and clinicians. This Usability Testing Plan shall detail the testing strategy, agreed-upon metrics and method of tracking, proposed timeline in the Contractors Management Plan and must be approved by VA Program Manager.

Deliverable:

A. Platform Access Tracker (iOS)
B. Usability Testing Plan

5.2.4 iOS Version Usability Testing

Once formal partnerships are in place, the Contractor shall then work with community hubs to enroll Veterans, following recruitment plan, and conduct user testing, following Usability Testing Plan, with the iOS version of the peer support group platform, including accompanying adjunct subclinical practice micro-learning library, to identify the most effective peer support group types (e.g., topics, duration, scheduling) and assess the effectiveness and usability of peer support groups sessions and psychoeducation in reducing stigma and other barriers to care, as well as any needed or recommended changes to the platform or enrollment process. Following completion of Usability Testing, the Contractor shall provide a Usability Testing and Feedback Report to the VA. The report should include plans for enhancements to the platform based on Veteran or clinician feedback. A minimum of 50 Veterans shall be enrolled for prototype and user experience testing for two initial community hubs. Veteran enrollment is subject to agreement to participate in usability testing and review and agreement to Cabana's End User License Agreement and associated privacy policies. If additional consent or formal agreement is needed to enable feedback sharing beyond what is captured in the platform, the Contractor shall create and provide operational Consent Form(s) for enrollees agreeing to complete usability testing of the Cabana Platform (iOS).

Deliverable:

A. Usability Testing and Feedback Report (iOS)
B. Operational Consent Form(s) for each participating Veteran, if needed

5.2.5 Feasibility Evaluation Design

The Contractor, in collaboration with partnered external evaluators, shall develop and refine the Feasibility Evaluation Design for Phase 2, aligned with the REAIM framework, and inclusive of a plan for any new prototype development, testing, and implementation (i.e. Android version of platform). Contractor shall provide the Phase 2 Evaluation Design and Testing Plan to the VA PM for approval.

Deliverables:

A. Phase 2 Evaluation Design and Testing Plan

5.2.6 Final Phase 1 Summary 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

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 18 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:

SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.3.1 Collaboration Agreements and Onboarding of Veteran Service Organizations

The Contractor shall develop and execute formal partnerships with a minimum of 3 additional community hubs/Veteran Service Organizations. Collaborator shall work with those enrolling Veterans in the Staff Sargent (SSG) Fox Suicide Prevention Grant Program at each of the identified VSOs and with their corollary VHA referral intake personnel. Contractor shall establish Memorandums of Understanding (MOU) with all collaborating VSOs, and other supporting organizations as needed, including external organizations supporting evaluation, and provide a report on those established partnerships.

Formal partnership shall include the Contractor onboarding the additional community hub staff to promote familiarity and ensure smooth adoption of the platform. Contractor shall conduct joint quarterly review sessions with Community Hubs and VA PM, and additional VA team members as designated, to monitor progress and document lessons learned. Contractor shall provide to VA meeting minutes from those quarterly all-party review sessions.

Deliverable:

A. MOU Report
B. Quarterly All-Party Review Session Minutes (6)

5.3.2 Development of Android Prototype of Platform and Usability Testing

Contractor shall complete development of Android prototype of Cabana platform. The Contractor shall then provide access to a digital library of on-demand, therapist-curated psychoeducation tools, and resources for self-guided microlearning (available twenty-four hours a day, seven days a week (24/7)), Cabana's Personalized Learning Journeys tailorable to individual users, and online live, professionally moderated peer support group sessions through the publicly downloadable Android version of the Cabana mobile application to all participants in this pilot with Android devices, including, but not limited to, Veteran patients, VSO stakeholders, Veterans Health Administration (VHÀ) Program, project staff and the acquisition contract support staff Contracting Officer's Representative (COR). The contractor shall maintain the software to include fixing defects, improving capabilities, and related functionality in support of the user community and VA, in addition to developing any needing training materials. Access to the Cabana Android platform shall be through Google Play and access for all parties above shall be confirmed by the Contractor and shared with VA through an Access Tracker as agreed upon by the VA Program Manager, including the minimum number of Veterans enrolled.

Contractor shall conduct usability testing with Android version of platform, following adapted Usability Testing Plan developed for iOS version in Phase 1, with at least 50 Veterans enrolled through any of the participating community hubs, and, once complete, will develop and provide to the VA a User Testing and Feedback Report. Contractor will then begin including Android version in feasibility, effectiveness, and scalability testing alongside iOS version of the platform.

Deliverable:

A. Platform Access Tracker (Android)
B. User Testing and Feedback Report (Android)

5.3.3 Sustainable Data Access and Analysis

The Contractor shall develop a means of accessing data metrics and analytics determined and approved in Phase 1 that will be accessible to both partnered community hubs and VA to enable joint, real-time monitoring of aggregate Veteran engagement and utilization of solution data as well as a count of VA referrals by community hub and associated VA site of care.

Contractor shall provide to VA a Monthly Data Analysis Report inclusive of data displayed by Community Hub or VA referral site.

Deliverable:

A. Project Data Access Resource
B. Monthly Data Analysis Report

5.3.4 Recruitment Strategy

Contractor shall iterate upon recruitment strategy development in Phase 1, in collaboration with prior and new community hubs, VA PM, and designated VA team members, to expand and enhance integration of Cabana into SSG Fox SPGP marketing and outreach activities at all participating community hubs. Contractor shall provide to the VA PM an updated Recruitment Strategy Plan for approval.

Contractor shall collaborate with all participating community hubs and VA to iterate on business processes and workflows for intra-network referrals, sign-ups, and crisis handoffs, as needed, co-determined by VA Program Manager, Contractor, and community hub representatives. Contractor shall provide to the VA PM an updated Referral and Enrollment Plan for approval.

Deliverable:

A. Recruitment Strategy Plan
B. Referral and Enrollment Plan

5.3.5 Platform Feasibility, Effectiveness, and Scalability Testing

Conduct feasibility, effectiveness, and scalability testing of iOS version, and Android version once available, including new enrollments of at least 1000 Veterans in total from all 5 community hubs (two from Phase 1 and three additional in Phase 2). Testing shall include development and implementation of any new technology enhancements based on Phase 1 feedback and any new Phase 2 feedback received from Veterans or clinicians during Android usability testing. Testing shall follow approved Phase 2 Evaluation Design and Testing Plan developed in Phase 1. At completion of testing, Contractor shall provide to the VA PM a Feasibility, Effectiveness, and Scalability Report.

Deliverable:

A. Feasibility, Effectiveness, and Scalability Testing Report

5.3.6 Sustainability and Scalability Plan

Contractor shall develop, in collaboration with VA PM, designated additional VA team members, and participating community hubs, a long-term sustainability and scalability plan for maintaining Cabana engagement and VA referrals plans across all 5 community hubs as well as engagement of additional community hubs. The Sustainability and Scalability Plan shall be provided to the VA PM for final review and approval.

Deliverable:

A. Sustainability and Scalability Plan

5.3.7 Final Project Summary Report

Contractor shall provide a Final Project Report, inclusive of a summary of all work from both Phase 1 and Phase 2, final data analyses of all agreed-upon metrics following

REAIM framework, and final value statement of solution implementation with recommendations for post-pilot sustainability and scalability.

Deliverable:

A. Final Project Summary 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☒	☐	☐
5.2	x☒	☐	☐
5.3	x☒	☐	☐

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).

Delivery Table

B.3 PRICE SCHEDULE

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 workday after the weekend or holiday.

BASE PERIOD					
LINE ITEM	DELIVERABLE	QTY	UNIT	UNIT PRICE	TOTAL
0001	**Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) Paragraph 5.1 inclusive of all subparagraphs.** **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**	**12**	**MO**	**Not Separately Priced (NSP)**	**NSP**

	Paragraph 5.1 inclusive of all subparagraphs. **Period of Performance (PoP) shall be 12 months** **Electronic submission to: VA Program Manager (PM), Contracting Officer Representative (COR) and Contracting Officer (CO).** **Inspection: destination** **Acceptance: destination**				
0001AA	Project Kickoff Meeting Agenda IAW PWS Paragraph 5.1.1 Due: Five days prior to the Technical Kickoff Meeting.	1	EA	NSP	NSP
0001AB	Project Kickoff Meeting Minutes IAW PWS Paragraph 5.1.1 Due: Three days after the Technical Kickoff Meeting	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
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
0002	**Initial Phase shall be provided IAW PWS Paragraph 5.2, and all 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 6 months from Date of Award** **Electronic submission to: VA PM, COR, and CO.** **Inspection: destination** **Acceptance: destination**				
0002AA	Collaboration Agreements from VA/and VSO IAW PWS Paragraph 5.2.1 Due 30 DAC award	1	EA	NSP	NSP
0002AB	Collaboration Agreements from VA/and VSO MOU report IAW PWS Paragraph 5.2.1 Due 30 DAC award	1	EA	NSP	NSP
0002AC	Collaboration Agreements from VA/and VSO Quarterly All-Party Review Session Minutes IAW PWS Paragraph 5.2.1 Due quarterly DAC Award	4	EA	NSP	NSP
0002AD	Recruitment Strategy Plan from VA/and VSO IAW PWS Paragraph 5.2.2 Due 60 DAC award	1	EA	NSP	NSP
0002AE	Referral and Enrollment plan from VA/and VSO IAW PWS Paragraph 5.2.2 Due 60 DAC award	1	EA	NSP	NSP
0002AF	Platform Access Tracker for (iOS) from Platform Access and Usability Testing Plan IAW PWS Paragraph 5.2.2 Due 60 DAC award	1	EA	NSP	NSP
0002AG	Usability Testing Plan from Platform Access and Usability Testing Plan	1	EA	NSP	NSP

	IAW PWS Paragraph 5.2.2 Due 60 DAC award				
0002AH	Usability Testing and Feedback Report (iOS) from iOS Version Usability Testing IAW PWS 5.2.4 Due 90 DAC award	1	EA	NSP	NSP
0002AI	Operational Consent Form(s) for each participating Veteran, if needed from iOS Version Usability Testing IAW PWS 5.2.4 Due 60 DAC award	1	EA	NSP	NSP
	Phase 2 Evaluation Design and Testing Plan from Feasibility Evaluation Design IAW PWS 5.2.5 Due 180 DAC Award	1	EA	NSP	NSP
	Final Phase 1 Summary Report From Final Phase 1 Summary Report IAW PWS 5.2.6 Due 180 DAC Award				
00003	**Initial Phase shall be provided IAW PWS Paragraph 5.3, and all its subparagraphs.** **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.** **Period of Performance (PoP) shall be DAC plus 6 months until plus 18 months Date of Award** **Electronic submission to: VA PM, COR, and CO.** **Inspection: destination** **Acceptance: destination**				
0003AA	MOU report from Collaboration Agreements and Onboarding of	6	EA		

	Veteran Service Organizations IAW PWS 5.3.1 Due 210 days from DAC Award				
0003AB	Quarterly All-Party Review Session Minutes from Collaboration Agreements and Onboarding of Veteran Service Organizations IAW PWS 5.3.1 Due 210 days from DAC Award	6	EA		
0003BA	Platform Access Tracker (Android) from Development of Android Prototype of Platform and Usability Testing IAW PWS 5.3.2 Due 240 days from DAC Award and then monthly through period of performance. To be part of monthly reporting.	17	EA	NSP	NSP
0003BB	User Testing and Feedback Report (Android) from Platform Access Tracker (Android) IAW PWS 5.3.2 Due 240 days from DAC Award and then monthly through period of performance. To be part of monthly reporting.	17	EA	NSP	NSP
0003CA	Project Data Access Resource from Sustainable Data Access and Analysis IAW PWS 5.3.3 Due 240 days from DAC Award and then monthly through period of performance. To be part of monthly reporting	17	EA	NSP	NSP
0003CB	Monthly Data Analysis Report from Sustainable Data Access and Analysis IAW PWS 5.3.3 Due 240 days from DAC Award and then monthly through period of performance. To be part of monthly reporting	17	EA	NSP	NSP

0003DA	Recruitment Strategy Plan from Recruitment Strategy IAW PWS 5.3.4 Due 210 days from DAC Award and then updated monthly through period of performance. To be part of monthly reporting	17	EA	NSP	NSP
0003DB	Referral and Enrollment Plan from Recruitment Strategy IAW PWS 5.3.4 Due 210 days from DAC Award and then updated monthly through period of performance. To be part of monthly reporting	17	EA	NSP	NSP
0003EA	Feasibility, Effectiveness, and Scalability Testing Report from Platform Feasibility, Effectiveness, and Scalability Testing IAW PWS 5.3.5 Due 510 days from DAC Award	1	EA	NSP	NSP
0003FA	Sustainability and Scalability Plan from Feasibility, Effectiveness, and Scalability Testing Report IAW PWS 5.3.6 Due 510 days from DAC Award	1	EA	NSP	NSP
0003GA	Final Project Summary Report from Final Project Summary Report IAW PWS 5.3.7 Due 510 days from DAC Award	1	EA	NSP	NSP
00004A		1	EA	NSP	Contractor Staff Roster IAW PWS Paragraph 6.2.2 Due 3 days after DAC award and updated within one day of any changes in employee status.
				TOTAL BASE PERIOD	

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	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	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	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	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 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 R*ights 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 contactor.

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.

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.

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.

   (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.

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.

   (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.

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.

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

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.

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