

VA



**U.S. Department
of Veterans Affairs**

**VETERANS HEALTH ADMINISTRATION (VHA)
DIGITAL HEALTH OFFICE (DHO)
OFFICE OF CLINICAL INFORMATICS (OCI)**

**VHA EHR Informatics Training Program (EITP) – Oracle Health Platform Advanced
Training**

**Date: May 7, 2026
PWS Version Number: 1.3**

STATEMENT OF WORK

Table of Contents

1.	INTRODUCTION	3
2.	APPLICABLE DOCUMENTS	3
3.	SCOPE OF WORK.....	3
4.	PERFORMANCE DETAILS	3
	4.1 PERFORMANCE PERIOD	3
	4.2 PLACE OF PERFORMANCE	4
	4.3 TRAVEL	4
5.	SPECIFIC TASKS AND SCHEDULE OF DELIVERABLES	4
7.	GOVERNMENT FURNISHED PROPERTY	8
8.	CONTRACTOR PERSONNEL SECURITY REQUIREMENT	8
9.	DELIVERY AND PACKING, INSPECTION/ACCEPTANCE REQUIREMENTS, WARRANTY:.....	8
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED	8
	APPENDIX C — VA INFORMATION AND INFORMATION SYSTEM SECURITY AND PRIVACY	11

1. **INTRODUCTION.** This document defines the materials, training, and support needed to provide advanced training on the Oracle Health Electronic Health Record (EHR) platform and associated tools to the Veterans Health Administration (VHA) for administration of Health Informatics roles and responsibilities.

1.1. Background. VHA provides informatics support for both the VistA-based and Oracle Health-based Federal EHR and associated tools to monitor VistA and Federal EHR use, configuration, and quality. VHA staff members who are or will be responsible for such support during and following the Federal EHR deployment require training on the Oracle Health platform and tooling architecture. This training is a discreet need from the VA-specific Oracle Health training provided to VHA staff at go live sites by VA's Electronic Health Record Modernization – Integration Office (EHRM-IO).

1.2. Oracle Health maintains a catalog of training opportunities available to VA's EHRM-IO and all Oracle Health clients. Training opportunities include instructor-led, virtual instructor-led, and self-paced online courses. Online courses range from 15 minutes to several hours. Instructor-led and virtual instructor-led courses range from 3 hours to 8 days. The training opportunities and catalog include per-course pricing ranging from approximately \$200 to \$4,850. Oracle Health also offers a "Premier Pass" option, which allows a holder of the "Premier Pass" to enroll in as many courses as they wish during the period of performance of the pass (typically, one fiscal year).

1.3. Additionally, there are two classes not included in the Premier Pass that are important to the informatics community, the Physician Architecture and Nurse Architecture classes.

2. **APPLICABLE DOCUMENTS.**

None.

3. **SCOPE OF WORK.**

The Contractor shall deliver platform-specific training regarding Oracle Health solutions and associated build and maintenance tools to VHA staff providing informatics support for the Federal EHR.

4. **PERFORMANCE DETAILS**

4.1 **PERFORMANCE PERIOD**

The period of performance (PoP) shall be 14 months from date of award. The overall Period of Performance shall not exceed 14 months.

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

on <https://www.opm.gov/policy-data-oversight/pay-leave/federal-holidays/#url=Overview>

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

Under current definitions, FIVE (5) are set by date:

New Year's Day	January 1
Juneteenth National	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 (6) are set for a day of the week and month:

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

4.2 PLACE OF PERFORMANCE

The tasks under this PWS shall be performed remotely, at the Contractor's site. The Contractor shall identify the Contractor's place of performance in their submission.

4.3 TRAVEL

The Government does not anticipate travel under this effort to perform the tasks associated with the effort.

5. SPECIFIC TASKS AND SCHEDULE OF DELIVERABLES

5.1. Oracle Health Platform-Specific Support Training.

5.1.1. Collaboration Kickoff.

- 5.1.1.1. The Government shall collaborate with the Contractor on defining an Oracle Health (OH) Certification plan for:
 - a. 2 OCI personnel through Premier Pass with period of performance ending on September 14, 2026
 - b. 28 OCI personnel through Premier Pass with period of performance of September 15, 2026 to September 14, 2027

- 5.1.1.2. The Government shall assist the Contractor in identifying and training a unique named points-of-contact (PoC) for set term including a primary and a back-up POC.
- 5.1.1.3. Provide OCI OH Utilization Report on a quarterly basis, aligning to OH financial quarters.
- 5.1.1.4. Provide dedicated, instructor-led courses, including remote and e-Learning.
- 5.1.1.5. Provide a training domain for all education classes that require a domain as delivered through this scope.
- 5.1.1.6. Provide access to the Client Education course catalog, which includes available courses, prerequisites, test-out options and policy.
- 5.1.1.7. Provide access for named POCs to OH Utilization reporting tools allowing POCs to monitor training activities such as enrollments, cancellations, and completions of VHA staff.
- 5.1.2. Premier Pass – across the Period of Performance (PoP) in this contract.
 - A. 2 Passes with period of performance ending on September 14, 2026
 - B. 28 Passes with period of performance September 15, 2026, to September 14, 2027
- 5.1.3. (OPTIONAL) Premier Pass – Not-To-Exceed (NTE) 20 passes across the Period of Performance (PoP) in this contract.
- 5.1.4. (OPTIONAL) Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate, Total Quantity: 60 participants; Five (5) Dedicated class for up to 12 enrollees each across the POP in this contract. This consists of two (2) separate offerings:
 - A. Millenium Architecture: Basic Physician
 - B. Millenium Architecture: Basic - Nurse
 - C. Physician Architect Program: Intermediate
 - D. Nurse Architect Program: Intermediate
- 5.1.5. (OPTIONAL) Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate, One (1) dedicated class for up to 12 seats across the POP in this contract. This consists of two (2) separate offerings:
 - A. Millenium Architecture: Basic – Physician
 - B. Millenium Architecture: Basic – Nurse
 - C. Physician Architect Program: Intermediate Education-
 - D. Nurse Architect Program: Intermediate Education
- 5.1.6. (OPTIONAL) Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate, , NTE 12 seats in Virtual Scheduled class (public with other OH customers), across the POP in this contract. This consists of two (2) separate offerings:
 - A. Millenium Architecture: Basic Education – Physician - Virtual
 - B. Millenium Architecture: Basic Education – Nurse - Virtual
 - C. Physician Architect Program: Intermediate Education - Virtual
 - D. Nurse Architect Program: Intermediate Education – Virtual

5.1.7. Training Materials. The Contractor shall deliver electronic copies of all training materials free from any constraints limiting maintenance, hosting, and distribution by VA.

Deliverables:

- A. OCI OH Utilization Report
- B. 2 Premier Passes
- C. 28 Premier Passes
- D. (OPTIONAL) – NTE 20 Premier Passes
- E. (OPTIONAL) NTE 60 participants; Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate, five (5) dedicated classes with up to 12 participants each class;
- F. (OPTIONAL) – NTE 12 participants; Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate one (1) dedicated class, up to 12 participants
- G. (OPTIONAL) – NTE 12 participants Physician Architect (PA) or Nurse Architect (NA) Program: Intermediate, in Virtual Scheduled class (public with other OH customers)

6. Delivery

6.1. As ordered by the government.

Task	Deliverable	Quantity	Delivery Date
Base Period			
5.1.1.3	OCI OH Utilization Report	4	Quarterly, after contract award, it is aligned to OH financial quarters. Electronic submission to: VA PM, COR, CO
5.1.2AA	Premier Pass (PP)	2	eLearning (Self-study or Instructor-Led)
5.1.2AB	Premier Pass (PP)	28	eLearning (Self-study or Instructor-Led)
5.1.3	OPTIONAL - PP	NTE 20	eLearning (Self-study or Instructor-Led)
5.1.4AA	OPTIONAL - Physician Architect (PA) Program: Millenium Architecture: Basic Intermediate, Five dedicated	60	eLearning

	classes for up to 12 enrollees each)		
5.1.4AB	OPTIONAL - Nurse Architect (NA) Program: Millenium Architecture: Basic Intermediate, Five dedicated classes for up to 12 enrollees each)	60	eLearning
5.1.4AC	OPTIONAL - Physician Architect (PA) Program: Intermediate, Five dedicated classes for up to 12 enrollees each)	60	eLearning
5.1.4AD	OPTIONAL - Nurse Architect (NA) Program: Intermediate, Five dedicated classes for up to 12 enrollees each)	60	eLearning
5.1.5AA	OPTIONAL - Physician Architect (PA) Program: Millenium Architecture: Basic	NTE 12	eLearning
5.1.5AB	OPTIONAL - Nurse Architect (NA) Program: Millenium Architecture: Basic	NTE 12	eLearning
5.1.5AC	OPTIONAL - Physician Architect (PA) Program: Physician Architect Program: Intermediate	NTE 12	eLearning
5.1.5AD	OPTIONAL - Nurse Architect (NA) Program: Nurse Architect Program: Intermediate	NTE 12	eLearning
5.1.6AA	OPTIONAL - Physician Architect (PA) Program: Basic Virtual scheduled class (public w/ other OH customers)	NTE 12	Virtual

5.1.6AB	OPTIONAL -Nurse Architect (PA) Program: Basic Virtual scheduled class (public w/ other OH customers)	NTE 12	Remote
5.1.6AC	OPTIONAL - Physician Architect (PA) Program: Intermediate Virtual scheduled class (public w/ other OH customers)	NTE 12	Virtual
5.1.6AD	OPTIONAL - Nurse Architect (NA) Program: Intermediate – Virtual scheduled class (public w/ other OH customers)	NTE 12	eLearning

7. **GOVERNMENT FURNISHED PROPERTY:** None.

8. **CONTRACTOR PERSONNEL SECURITY REQUIREMENT:** None

9. **DELIVERY AND PACKING, INSPECTION/ACCEPTANCE REQUIREMENTS, WARRANTY:** Electronic Delivery

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.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with 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.

A3.0 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): https://www.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): https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A4.0 Notice of the Federal Accessibility Law Affecting All Information and Communication Technology (ICT) Procurements (Section 508)

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

A4.1. Section 508 – Information and Communication Technology (ICT) Standards

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>. A printed copy of the standards will be supplied upon request.

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

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

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

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☐ E206 Hardware Requirements
- ☐ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

A4.2. Compatibility with Assistive Technology

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

A4.3. Acceptance and Acceptance Testing

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

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

A5.0 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.

APPENDIX C — VA INFORMATION AND INFORMATION SYSTEM SECURITY AND PRIVACY

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

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

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

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

the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

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

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:
 - (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.

5. SECURITY INCIDENT INVESTIGATION.

A 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 employees shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.
- d. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.
- e. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation

from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

- f. The contractor shall comply with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.
- g. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.
- h. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated damages to the VA as set forth in clause [852.211-76, Liquidated Damages— Reimbursement for Data Breach Costs](#).

6. NOT APPLICABLE

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.
- 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.

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:
 - (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.

13. NOT APPLICABLE

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.