Consolidated Patient Account Center [CPAC] Revenue Operations [RO]

Performance Work Statement [PWS]

Indefinite Delivery Indefinite Quantity [IDIQ]

Insurance Entry and Verification Buffer Support Services

1.0 SCOPE

The Contractor shall provide all labor, supervision, management, equipment, and other resources necessary to perform insurance entry and verification services for the Department of Veterans' Affairs [VA] patient insurance information in authorized VA healthcare systems for CPAC sites nationwide.

2.0 BACKGROUND

The VA has historically relied on contract support to improve collections and information integrity through timely and accurate entry and verification of third-party insurance information. The VA's CPACs are responsible for ensuring accurate and current insurance documentation for medical treatment provided to veterans for non-service-connected [NSC] conditions. Insurance entry and verification services include the identification, establishment, update, termination, sequencing, resequencing, and coordination of benefits for medical and prescription insurance policies using authorized methods and systems.

2.1 There are seven [7] regional CPACs located as follows:

Number	Location	Name	Abbreviation
Station 730	Asheville, NC	Mid-Atlantic CPAC	MACPAC
Station 731	Smyrna, TN	Mid-South CPAC	MSCPAC
Station 732	Middleton, WI	North Central CPAC	NCCPAC
Station 733	Orlando, FL	Florida Caribbean CPAC	FCCPAC
Station 734	Lebanon, PA	Northeast CPAC	NECPAC
Station 735	Leavenworth, KS	Central Plains CPAC	CPCPAC
Station 736	Las Vegas, NV	West CPAC	WCPAC

2.2 VA is currently undergoing organizational changes that may result in future adjustments to structure, processes, responsibilities, and priorities. Such changes may affect the customers, services, and support described in this PWS. The Contractor shall remain capable of supporting evolving VA requirements as directed through the contract or applicable Task Order. Any resulting change to contract scope, schedule, or other terms shall be effected only through bilateral contract modification, as applicable.

2.3 Public Law 99-272 grants VA authority to seek reimbursement from third-party health insurers for the cost of medical care furnished to an insured NSC veteran. Public Law 101-508 expanded VA's recovery program by providing authority to seek reimbursement from third-party payers for the cost of medical care provided to service-connected veterans treated for NSC conditions.

DRAFT

3.0 OBJECTIVES

The objective of this PWS is to obtain insurance entry and verification services that result in accurate, timely, and compliant establishment, updating, verification, and maintenance of third-party insurance information for CPAC sites nationwide. Contractor performance shall be evaluated based on required results, measurable performance standards, and the Government's quality assurance surveillance methods identified in this PWS and the Performance Requirements Summary Matrix [PRSM].

4.0 TASKS AND DELIVERABLES

The Contractor shall provide services necessary to establish, update, and verify insurance entries for veterans and their third-party insurance carriers within authorized VA systems and associated software interfaces in accordance with applicable VA policies, procedures, and Task Order requirements. The Government's required outcome is the timely completion of accurate and compliant insurance entries and related actions necessary to support CPAC operations. Except where specific constraints are stated in the contract, the Contractor is responsible for determining the methods, staffing approach, and internal processes used to achieve the required results. Performance shall be measured in accordance with **Section 12.4**, Performance Requirements Summary Matrix, and monitored through the Government's Quality Assurance Surveillance Plan [QASP].

4.1 Deliverable – Entry and Verification of Insurance Information

The Contractor shall complete insurance entry and verification services in a manner that produces accurate, timely, and compliant records in accordance with CPAC guidebooks, VA policy, and Task Order requirements. Required performance levels for this deliverable are set forth in **Section 12.4**.

4.1.1 TIMELY COMPLETION OF INSURANCE ENTRY AND VERIFICATIONS:

All assigned insurance entries and verifications shall be completed within the delivery period established by the applicable Task Order and at the performance level stated in **Section 12.4**.

4.1.2 DATA ENTRY ACCURACY:

Insurance entries shall be accurate, complete, and processed in accordance with CPAC guidebooks, VA policy, and Task Order requirements at the performance level stated in **Section 12.4**.

4.1.3 RESOLVING INSURANCE ENTRY REJECTIONS:

The Contractor shall review and take required action on erroneous or rejected insurance entries within the timeframes established in **Section 12.4** and the applicable Task Order.

4.1.4 RESOLVING INSURANCE ENTRY RELATED QUESTIONS AND CONCERNS:

The Contractor shall provide timely and effective communication necessary to resolve insurance entry questions, discrepancies, and concerns related to contract performance. Performance shall be evaluated in accordance with **Section 12.4**.

DRAFT

4.1.5 CONFERENCE CALL PARTICIPATION:
The Contractor shall participate in Government required conference calls or meetings necessary to support contract performance and issue resolution, as identified by the COR or Task Order requirements. Performance shall be evaluated in accordance with **Section 12.4**.

4.1.6 MAINTAIN VA SYSTEMS AND PROVIDER PORTAL ACCESS:
The Contractor shall maintain the access necessary to perform assigned work in authorized VA systems and assigned insurance provider portals without interruption that would adversely affect required performance outcomes. The Contractor is responsible for managing its workforce and internal processes to maintain performance at the levels set forth in **Section 12.4**.

4.1.7 CONFIDENTIALITY:
The Contractor shall perform all insurance entry and verification services in compliance with applicable privacy, confidentiality, and information security requirements and at the performance level stated in **Section 12.4**.

4.2 Deliverable – Monthly Itemized Statement – Not Separately Priced
The Contractor shall provide an itemized statement monthly to the CPAC Insurance Verification Manager and COR outlining the insurance entries completed, rejected entries, and any access issues or performance issues encountered in performance of this task. Monthly reports, due by the fifth day of each month unless otherwise specified in the Task Order, shall include, at a minimum:

4.2.1 Summary of quantity of insurance entries completed per facility per reporting period, and cumulative for the contract to date.

4.2.2 Number of entries completed per staff member.

4.2.3 Unit price and total cost of insurance entries completed, if applicable to the pricing structure.

4.2.4 Number of entries rejected.

4.2.5 Unit price and total cost of entries rejected, if applicable for deduction in accordance with the contract.

4.2.6 Number of entries per CPAC, broken down per staff member and per VA Medical Center [VAMC].

4.3 Deliverable – Monthly Staffing Report – Not Separately Priced
The Contractor shall develop and submit a Monthly Staffing Report to the CPAC Insurance Verification Manager and COR, due by the fifth day of each month unless otherwise specified in the Task Order. The report shall include staff hired for performance under this contract, staff no longer performing under this contract, anticipated start or termination dates, and assigned primary CPAC facility.

DRAFT

4.3.1 Electronic copies shall be delivered submitted in a format acceptable to the COR, unless otherwise specified in the Task Order.

4.3.2 The Contractor shall provide staff with training and updates necessary to maintain performance in accordance with current applicable policies, procedures, and regulations relevant to the services required under this contract. Tracked updates and training provided to staff shall be included in the monthly staffing report, as applicable.

4.4 Deliverable – Weekly Pending Workload Report – Not Separately Priced

The Contractor shall develop and submit a Weekly Pending Workload Report to the CPAC Insurance Verification Manager and COR, due by Monday of each week unless otherwise specified in the Task Order. The report shall include facility, received date, and remaining insurance entries for VA Care and Community Care sufficient for the Government to monitor workload status and timeliness.

4.4.1 Electronic copies shall be submitted in a format acceptable to the COR, unless otherwise specified in the Task Order.

4.5 Performance Measurement

Unless otherwise stated in the applicable Task Order, the Contractor's performance under this section shall be assessed using the indicators, standards, acceptable quality levels, and surveillance methods set forth in **Section 12.4**, Performance Requirements Summary Matrix.

5.0 FORMAL ACCEPTANCE OR REJECTION OF DELIVERABLES

All written deliverables shall be clear, organized, and suitable for Government review and use. The Contracting Officer's Representative [COR] may reject or require correction of deficiencies found in the deliverables. In the event of a rejected deliverable, the Contractor shall be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five [5] workdays to correct the rejected deliverable and return it in accordance with delivery instructions, unless otherwise directed by the COR or Task Order. If any deliverable cannot be provided within the scheduled timeframe, the Contractor shall notify the COR in writing by the delivery due date, explain the reason for the delay, describe the impact, and provide a firm commitment date for completion. The COR will forward the notice to the Contracting Officer [CO] with comments, and the CO will respond in accordance with the contract and applicable regulations.

The Contracting Officer's Representative [COR] is the Government official designated in writing by the Contracting Officer to perform specific technical, functional, and oversight responsibilities for this contract, including inspection and acceptance of services and deliverables within the limits of that delegation.

5.1 Acceptance Criteria

Government acceptance of services is contingent upon the Contractor's performance meeting the applicable requirements of this contract and the measurable performance standards identified in **Section 12.4**.

DRAFT

5.2 Government Acceptance Period

The COR will have ten [10] business days to review draft deliverables and provide comments, unless otherwise stated in the contract or Task Order. The Contractor shall have five [5] business days to make required corrections, unless otherwise directed. Upon receipt of final deliverables, the COR will have two [2] business days for final review prior to acceptance or providing documented reasons for non-acceptance. If the Government does not complete review within the stated review period, the deliverable may be treated in accordance with the applicable inspection and acceptance terms of the contract.

6.0 COMMUNICATION REGARDING INSURANCE ENTRY ISSUES

Direct communication regarding insurance entry issues should be addressed to the Insurance Verification Manager or Supervisor, as identified by the Government after award.

7.0 PERFORMANCE DETAILS

7.1 Indefinite Delivery Indefinite Quantity [IDIQ] Period of Performance: Sixty [60] month ordering period.

7.2 Periods of performance and quantities shall be established for each Task Order.

7.3 Eleven [11] Federal holidays set by law under U.S.C. Title 5 Section 6103 apply.

New Year's Day	January 1
Birthday of Martin Luther King Jr.	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth Independence Day	June 19
Independence Day	July 4
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11
Thanksgiving Day	Fourth Thursday in November
Christmas Day	December 25

7.3.1 If a federal holiday falls on a Saturday, the holiday is observed on the preceding Friday. If a federal Holiday falls on a Sunday, the holiday is observed on the following Monday.

7.4 Place of Performance

The place of performance shall be the responsibility of the Contractor. No Government space will be provided by CPAC unless otherwise specified in the contract or Task Order. The Contractor shall provide a remote, secure business environment suitable for healthcare insurance information entry and verification and shall maintain patient confidentiality and data security at all times.

DRAFT

7.5 Hours of Operation

The normal operating hours for the Federal Government are Monday through Friday, 8:00am to 4:30pm local area time. VA and CPAC employees shall be able to communicate with the Contractor's key personnel from 8:30 am to 5:00 pm Eastern Time [ET] during federal workdays unless otherwise specified by the contract or Task Order.

8.0 ORDER TERMS, CONDITIONS, AND PROVISIONS

8.1 Rejections

If an insurance policy cannot be loaded into VistA and/or linked appropriately, the matter shall be transferred to the appropriate CPAC contact for further review and resolution at no charge to the Government. VA estimates that 10 to 15 percent of daily workload may result in such rejections.

8.2 Non-Disclosure/Non-Use Agreement

The Contractor shall ensure that each Contractor employee completes a Non-Disclosure/Non-Use Statement before performing any work under this contract. The Non-Disclosure/Non-Use Statement shall be cosigned by a corporate official at the Contractor Task Manager level or higher and provided to the COR.

9.0 INFORMATION ASSURANCE

9.1 General Security Requirements

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect Government data and ensure the confidentiality, integrity, and availability of such data. As a minimum, this shall include personnel security, electronic security, and physical security measures as required by this contract.

9.2 HIPAA

The Contractor shall comply with the applicable requirements of the Health Insurance Portability and Accountability Act of 1996 [HIPAA].

10.0 PROTECTION OF INFORMATION

10.1 Dissemination of Information/Publishing

The Contractor shall not disseminate or publish VA insurance information, policies, or tools except as authorized by this contract or by the Contracting Officer.

10.2 Personally Identifiable Information (PII) and Protected Health Information (PHI)

The Contractor shall comply with all applicable privacy and security requirements governing PII and PHI in performance of insurance entry and verification services.

11.0 CONTRACTOR EXPERIENCE REQUIREMENTS

11.1 Key Personnel

Key personnel are those individuals identified by the Contractor and accepted by the Government for performance of critical contract functions. Such personnel shall possess

DRAFT

demonstrated experience managing insurance entry and verification operations with similar scope, complexity, and volume to the work described in this PWS. The CO may require removal of any Contractor-assigned individual whose performance is unsatisfactory or whose continued performance presents a conflict of interest or other concern to the Government. Replacement personnel shall be identified within three [3] business days of notification unless otherwise approved by the CO. Employment or staffing difficulties shall not excuse failure to meet contract requirements.

11.2 Substitution of Key Personnel

All Contractor requests for substitution of key personnel shall be submitted in writing to the COR and CO at least thirty [30] calendar days before the proposed effective date whenever practicable. Requests shall include an explanation of the circumstances necessitating the substitution, a complete resume for the proposed substitute, and any other information required by the CO to approve or disapprove the substitution. New personnel shall not begin work in a key position until required security requirements have been satisfied and the proposed substitute has been accepted by the Government, if such acceptance is required by the contract.

11.3 Management and Oversight

The Contractor shall be responsible for managing and overseeing the activities of all Contractor and subcontractor personnel performing under this contract. Contractor management responsibilities include all actions necessary to ensure timely and effective performance in accordance with the requirements of this PWS and applicable Task Orders.

11.4 Domain Knowledge

The Contractor shall demonstrate domain knowledge of outpatient healthcare insurance entry and verification operations relevant to the services required under this PWS.

11.5 Training

The VA will train the Contractor's key personnel, including managers and supervisors, on VA VistA and related applications necessary for insurance entry and verification, as applicable. The Contractor shall ensure its personnel are adequately trained to perform the required services in accordance with contract requirements.

11.6 Standards of Conduct

The Contractor shall ensure that personnel assigned to this contract comply with the Standards of Ethical Conduct at 5 CFR 2635. Personnel assigned by the Contractor to perform work shall be acceptable to VA in terms of personal and professional conduct and technical knowledge. The CO may notify the Contractor and require immediate removal of any contractor personnel determined to be unacceptable in terms of technical competency or personal conduct. The Contractor shall remove and replace such personnel at no additional cost to the Government. Replacement personnel qualifications shall be equal to or greater than those of the personnel being replaced. Employment and staffing difficulties shall not justify failure to meet established schedules.

DRAFT

11.7 Utilization of Government Employees

The Contractor shall notify the CO whenever an employee of the United States Government is utilized by the Contractor in performance of the contract. The notification shall include sufficient information for the CO to review the matter in accordance with applicable FAR conflict of interest requirements.

11.8 Staff Qualifications

11.8.1 General Experience:

Contractor personnel assigned to this contract shall have expertise in performing insurance entry and verification services relevant to the work required under this PWS.

11.8.2 Managers and Supervisors:

Managers and supervisors shall have relevant knowledge and experience within the past five [5] years in insurance entry and verification operations. This experience should reflect subject matter expertise in identifying, loading, sequencing insurances and resolving complex insurance files. Experience leading and managing workload and staffing within the past five [5] years is preferred.

12.0 QUALITY ASSURANCE

12.1 Contractor Quality Assurance

The Contractor shall conduct internal quality reviews of completed insurance entries sufficient to support performance at or above the required standards of this contract.

12.2 Government Quality Assurance

The Government, including external auditors as applicable, may conduct periodic independent quality reviews of the Contractor's insurance entry work. Findings may be provided to the COR and Contractor for review and corrective action, as appropriate.

12.3 Quality Assurance Surveillance Plan [QASP]

The Government intends to utilize a Quality Assurance Surveillance Plan [QASP] to monitor the quality of Contractor performance and to help ensure that service levels meet and maintain required standards for insurance entry and verification services. The QASP provides the COR with a means to identify unacceptable or deficient performance and provides verifiable input for Contractor Performance Assessment Reporting System [CPARS] evaluations, as applicable. The QASP will be finalized following award and provided to the Contractor. The QASP is a living document and may be updated by the Government as necessary in accordance with the contract.

12.4 Performance Requirements Summary Matrix

By monitoring the Contractor, the COR will determine whether the performance levels set forth in the order have been attained. Performance standards are specified in the following Performance Requirements Summary Matrix in the Standard and Acceptable Quality Level columns.

DRAFT

TASK	INDICATOR	STANDARD	ACCEPTABLE QUALITY LEVEL [AQL]	METHOD OF SURVEILLANCE
4.1.1	Timely completion of insurance entry and verification	Insurance entries are completed within the period assigned by the CPAC or the applicable Task Order	≥93% on-time completion	Review of VA CPAC QA documents or periodic inspection
4.1.2	Data entry data accuracy	Insurance entries are performed in accordance with CPAC guidebooks and VA policy	Individual data entry quality review does not fall below 95%	Review of VA CPAC QA documents or periodic inspection
4.1.3	Resolving insurance rejections	Rejected insurance entries are reviewed and actioned within required timeframes	100% review and action taken on rejected entries within 5 business days	Review of QA documents
4.1.4	Resolving insurance entry questions and concerns	Clear communication is provided for timely resolution	No more than three [3] validated communication failures per quarter	Validated user complaints
4.1.5	Conference call participation	Contractor participates in required calls or meetings	No more than two missed calls per rating period; 100% Contractor leadership or designee attendance when required	Validated attendance lists
4.1.6	Maintain VA Systems and Provider Portal Access	Contractor maintains access necessary to perform assigned work	No more than one access reset per month attributable to Contractor failure to maintain access	Validated requests to regain access
4.1.7	Confidentiality maintained in entries	Entries comply with VA privacy and security requirements	No substantiated violations of VA privacy or security requirements	Revenue Operations Privacy Officer or other designated Government review

13.0 VA INFORMATION AND INFORMATION SYSTEM SECURITY AND PRIVACY LANGUAGE

13.1 General

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.

13.2 VA Information Custodial Language

DRAFT

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General. The primary clause used to define computer software license (not data/intellectual property first produced under this Contractor or order) is FAR 52.227-19, Commercial Computer Software License.

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

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

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

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

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

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

DRAFT

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.

DRAFT

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that are 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 VA CO.

13.3 Access to VA Information and VA Information Systems

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

b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 13.4, 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 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

DRAFT

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 have a need for access to VA information or VA information systems.

    2. Contractor/subcontractor personnel are terminated, suspended, or otherwise have 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 access 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

DRAFT

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

13.4 Training

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

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

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

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

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

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

13.5 Security Incident Investigation

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

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

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

DRAFT

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

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

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

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

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

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

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

e. In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

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

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

h. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving

DRAFT

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.

13.6 Data Center Provisions

The Contractor shall comply with applicable VA and Federal network, infrastructure, continuity, and boundary protection requirements relevant to any systems or environments used in performance of this contract.

a. The Contractor shall ensure the VA network is accessed 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.

DRAFT