SCOPE OF WORK

The Contractor shall develop a software product, which will modify existing VistA software to allow pharmacies at OneVA locations to make changes and address prescriptions through a middleware model that meets VA standards and removing controlled substances from the active refill list. The Contractor shall provide all documentation, complete all testing activities, and training for the product in accordance with an IOC delivery of the capability. The contractor will provide a tailored set of PMAS documents consistent with the identified approach. The contractor and the government will agree to specific PMAS modifications in the first 30 days of the project.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (POP) shall be 6 months from the date of award.

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

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Page 21 of 65

VA118-15-F-0663

Under current definitions, four are set by date

New Year's Day Independence Day Veterans Day Christmas Day

January 1 July 4 November 11 December 25

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

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

Martin Luther King's Birthday January Washington's Birthday February Memorial Day

Labor Day Columbus Day Thanksgiving

4.2 PLACE OF PERFORMANCE

Third Monday in Third Monday in

Last Monday in May First Monday in September Second Monday in October Fourth Thursday in November

Tasks under this PWS shall be performed at Contractor facilities.

4.3 TRAVEL

Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

For informational purposes, the total estimated number of trips in support of this effort is two. Anticipated locations include the following, estimated at 5 days in duration:

Planning Lockdown: Washington, DC Testing: Denver, CO

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Project Management Plan (PMP) that lays out the Contractor’s approach, timeline, and tools to be used in execution of this Task Order effort. The PMP should take the form of both a narrative and graphic format that

Page 22 of 65

VA118-15-F-0663

displays the schedule, milestones, risks, and resource support. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline PMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved PMP throughout the period of performance. Contractor shall use the PMP modified template approved for use in ProPath. ProPath modified templates are subject to change through the lifecycle of the project and the contractor will be responsible for ensuring the most current modified template is applies and used.

The schedule and risks reported in the PMP should be provided as separate documentation in the form of a project schedule and a risk issue log. The project schedule must meet minimum requirements established by ProPath and PMAS, and the contractor will be required to access Primavera where the project schedule is required to be maintained. The Risk Issue Log modified template is available through ProPath.

The Contractor shall coordinate and facilitate a kick-off meeting and shall provide an agenda within 5 business days after contract award. An entrance conference kick-off meeting shall be held at virtually within 10 business days after the contract has been awarded.

Deliverables:

A. Project Management Plan B. Kick-offMeeting C. Primavera Project Schedule D. Risk Issue Log

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the Contracting Officer’s Representative (COR) with Monthly Progress Reports in electronic form in Microsoft Word format. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month. The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the PMP and project schedule and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that

arise are transparent to both parties to prevent escalation

Deliverables:

A. Monthly Progress Report B. Progress Meeting Minutes C. Updated Primavera Project Schedule

of outstanding issues.

Page 23 of 65

VA118-15-F-0663

D. Updated Risk Issue Log

5.1.3 CODE IN FLIGHT (CIF)

OI&T senior leadership mandated submission to the CIF program with ProPath v13, released September 19, 2012.

All development products/projects have a requirement to provide multiple copies as the software matures through development phases. The defined points in ProPath are mandatory submission points, but the higher the frequency of follow-on submissions, the more likely you are to get good feedback from the open source community. The goal of CIF is to share early and often. Products must release to Open Source, Configuration & Tools Management (OSCTM) Division at least once perPMASiteration, withfollowoncyclicalsubmissionsfornewproductbuilds.

Every 6 months, or at least once per PMAS increment (whichever occurs sooner), the Contractor shall submit the full body of your code including both software and data/data definitions formatted into a build, along with all software engineering and user documentation as it currently exists AS IS, including both Class 3 and software maturing into C1 code/documents.

OSCTM will review it for FOIA redaction of commercial and secured/sensitive content components (if any), and we will follow the CIF program policies to release it to open source.

The Code in Flight may be submitted to OSEHRA. More information regarding OSEHRA can be found by visiting the following link: http://go.va.gov/opensource.



5.1.4

A. Deliverables: Open Source Code In Flight Submission Project Coordination and Integration

5.1.4.1 VistAPatchCoordination

The contractor must attend and participate in weekly VistA Patch Coordination meetings with other development groups that may help to identify code dependencies between projects. The contractor will be required to input VistA patch information into FORUM and keep this information updated.

5.1.4.2 IntegratedProjectTeam(IPT)

The contractor must coordinate with numerous stakeholders as well as other Program Offices and Projects to include VA’s Enterprise Messaging Infrastructure (eMI), VistA Interface Engine (VIE) and Clinical Data Services (CDS) to ensure the new solution can meet the Software Development Requirement below to remove the Rx Manager component of the prototype. In order to ensure the best solution can be achieved to fit within the project timelines, the contractor will attend and participate in weekly Project IPT Meetings and be responsible for capturing meeting minutes that include the

Page 24 of 65

VA118-15-F-0663

attendees present at each meeting, approval of previous meeting minutes, and relevant information exchanged on the call. Contractor will also prepare agenda items from participating IPT members priorto eachmeeting.

5.1.4.3 ProjectDailyStandUpCall

The contract will establish and maintain a 15-30 minute daily stand up call to review progress of Tasks assigned to individuals in RTC. The purpose of these short daily calls is to quickly review with each team member which task was worked the previous day, which task will be worked the current day and to identify obstacles the team member has that is keeping them from completing any assigned task. These calls allow the Contractor PM as well as the VA PM to quickly assist in removing impediments for the team and to identify potential risks to the project schedule.

Deliverables:

A. IPT Meeting Minutes B. Daily Stand Up Call Meeting Minutes

5.2 SOFTWARE DEVELOPMENT PLANNING

Prior to beginning development of the solution, the Contractor shall perform the following:

1. Ensure the full body of Functional and Non-Functional Requirements are identified through the various project stakeholders (identified in the project Business Requirement Document) and documented in both VA’s Rational Requirements Composer (RRC) and a project Requirements Specification Document (RSD) that meets ProPath modified template requirements.
2. Obtain signature of RSD through various project stakeholders identified in

the RSD modified template.

1. Create Epics, User Stories, and Tasks (development, documentation, and testing) in VA’s Rational Tools Composer (RTC) that correlate to the requirements to ensure the full body of work to be performed is captured at the task level and that tasks are no larger than 8 hours of work.
2. The solution for each development task should be documented and populated into the System Design Document (SDD) to present the solution design to stakeholders and other review boards (such as the Architecture and Engineering Review Board and other required OI&T Service Delivery and Engineering reviews). The SDD ProPath modified template must be used for this required document.
3. The Contractor will complete the following items to ensure the project can proceed ETA Compliance Checklist (link to ETA Compliance Checklist here: http://vaww.oed.wss .va.go v/p rocess/Library/e ta\_compliance\_c heck list\_temp late.htm)  These documents are: SDD RSD All C&A/A&A documentation (Contingency Plan, Disaster recovery, System

 

Page 25 of 65

VA118-15-F-0663

Security Plan, ATO, etc. anything at the link below with AAA as the process ID) Operational Acceptance Plan Production Operations Manual

Deliverables:

A. Requirements Specification Document (RSD) B. RRC and RTC Entry of requirements, user stories and tasks with proper

links established C. System Design Document (SDD)

5.3 SOFTWARE DEVELOPMENT 5.3.1 Software Requirements

Upon completion of development planning, the Contractor shall perform the following software development efforts:

1. Modify the existing system such that upon the selection of active-refillable prescriptions that are controlled substances a message is displayed to inform the user that the prescription selected cannot be refilled and terminate the request.
2. Modify drug matching functionality in prototype to require VA Product to find a match.
3. Modify the current platform to display the entire medication profile from other VA pharmacies by utilizing data from Clinical Data Service (CDS) while maintaining the existing requirement to develop and demonstrate the exchange of patient sensitive information between systems in a secure manner in accordance with VA regulations for Privacy and Security.
4. Remove the existing prototype requirement to lock out any remote site user from taking action on a patient’s prescriptions while the information is being accessed and/or actioned by the local VA site. Remove the existing prototype requirement to provide the ability for VistA to time out the local site pharmacy user after 5 minutes of inaction, freeing up the patient’s medication profile for action by the remote site again.
5. Develop solution to eliminate Rx Manager by utilizing the Enterprise Messaging Infrastructure (eMI) and VistA DHCP Health Level 7 while maintaining the existing requirement to develop and demonstrate the exchange of patient sensitive information between systems in a secure manner in accordance with VA regulations for Privacy and Security.
6. Update all previously delivered PMAS Documentation during and post development to keep technical documentation current for required PMAS Reviews such as Operational Readiness Review, Initial Operating Capability Entry and Exit, and preparation for National Deployment.
7. Provide defect fixes that result from functional, user, operational readiness and initialoperatingcapabilitytesting.
8. Update and/or create any remaining documentation required for Initial Operating Capability (IOC) documentation and National Release. The Contractor will complete the following items to ensure the project can proceed

Page 26 of 65

VA118-15-F-0663

Enterprise Release Management will update the documents listed in 5.2 in addition to Release Registration, Testing Intake, CP&E and ASSESS forms. Additional forms that may be required for ESE Release Review/Operational Readiness may need to be completed:

http://vaww.oed.wss .va.go v/p rocess/Web\_Pages/required\_pro ject\_prod uct\_a rt

ifacts.aspx 9. This is not an exhaustive list of required documentation, as some will

additionally be listed under PWS Section 5.4 Testing and 5.5 Deployment. 10.Ensure developers update all development related RTC tasks assigned to

them.

Deliverables:

A. Approved Source Code B. Updated and Approved ProPath Required Documentation C. Required and Approved ProPath IOC Documentation

5.4 TESTING 5.4.1 Planning

The Contractor shall be responsible for performing all unit, software quality assurance (SQA) and coordinating and preparations for user, operational readiness(OR)andinitialoperatingcapabilitytesting(IOC). Eachphaseof testing requires documentation and planning. This planning can and should run concurrent with development planning. As such, the contract shall:

1. Ensure all required testing related artifacts required by PMAS and ProPath are drafted, to include: Master Test Plan, Test Cases and Test Scripts, Requirements Traceability Matrix, VistA Software Quality Assurance Checklist,HealthProduct SupportEnterpriseApplicationCompletionand Release Checklist, IOC Entry Request and Exit Summary, IOC Site Evaluation Defect Log and Concurrence Statement, IOC Site Memorandum of Understanding, and IOC Testing Waiver (if applicable).
2. Obtain signatures for Master Test Plan
3. Create Tasks related to testing and testing documentation in VA’s Rational  Tools Composer (RTC) that correlate to either functional requirements and/or development tasks to ensure the full body of work to be performed is captured at the task level and that tasks are no larger than 8 hours of work.
4. Ensure all Test Cases and Test Scripts are reviewed by developers, testers and end users to assure accuracy and usability.
5. Identity a minimum of three test sites to participate in user functional and IOC testing and obtain signatures from those sites for the IOC Site Memorandum of Understanding
6. Ensure the Operational Readiness Review process is initiated and that all documentation required for this review is up-to-date and submitted. The contractor shall track the review process and respond to any questions and/or updates required by the review team and incorporate them into the Master Test Plan.

 

Page 27 of 65

VA118-15-F-0663

Deliverables:

1. Signed Master Test Plan
2. Peer and User Reviewed and Approved Test Cases and Test Scripts
3. Testing Related Tasks Entered into RTC
4. Signed IOC Site Memorandum of Understanding
5. Risk Analysis and Testing Scope Report (RATSR) results incorporated  into Master Test Plan

5.4.2 Unit Functional Testing

The Developer performs Product Component Testing (aka Unit Testing) which includes the internal technical and functional testing of a module/component of code and is responsible that the verification of the requirementsdefinedinthe detaileddesignspecificationhavebeen successfully applied to the module/component under test. Unit testing will require developers to:

- Analyze requirements to understand the application functionality and dependencies - Identify all the routines affected by the module or object - Specify all the routines that are called from various locations

- Execute tests on prioritized options - Execute tests with different combinations of options and data. For example, test with minimal data entered and test with maximal data entered - Perform exploratory testing, i.e., randomly exercise the module, object, and options based upon domain knowledge, past performance, and expertise - Record the actual test results - Perform static analysis of module/component source

code As such, the contractor shall:

1. Ensure each developer tests the full functionality of the code they are developing to assure the code meets the Requirements Specification Document and to assure the code they develop does not adversely impact existing software functionality.
2. Ensure each unit test has a completed Primary Developer Checklist and Second Developer Checklist and that these checklists are provided to SQA testers with draft builds to be tested.
3. Ensure all code that is not MUMPS code developed for the solution has been scanned using the HP Fortify Static Code Analyzer and that all deficienciesare remediated,
4. Ensure developers update all related RTC tasks they are assigned for Unit Functional Testing.  Deliverables:

A. Primary Developer Checklists B. Secondary Developer Checklists

C. Updated and Approved Test Cases and Test Scripts and Results

Page 28 of 65

VA118-15-F-0663

1. HP Fortify Static Code Analyzer Scan Results
2. Product Build for SQA Testing

5.4.3 Software Quality Assurance (SQA) Testing

The Contractor shall be responsible for performing all software quality assurance (SQA) testing that tests the front and back-end functionality of the remediated application per the Requirements Specification Document, but ensures the product is regression tested as defect fixes occur and that the product is truly ready for end user testing in a test site test account. As such, the contract shall:

1. Ensure each SQA tester test the code using approved Test Cases and Test Scripts and that each test is passed or failed according to the documented pass/failcriteria.
2. Ensure SQA test cases and scripts and test results are captured and correlated to the appropriate functional requirements, tasks and/or user stories in the Requirements Traceability Matrix.
3. Ensure for each product build tested, a Test Evaluation is created.
4. Ensure for each product build tested that SQA testers complete the  VistA Software Quality Assurance Checklist.
5. Ensure testers update all related RTC tasks they are assigned for Unit  Functional Testing.  Deliverables:
6. Updated Test Cases and Test Scripts and Results
7. Updated Requirements Traceability Matrix
8. Product Build Test Evaluations
9. Product Build VistA SQA Checklists

5.4.4 User Functional Testing

The Contractor shall be responsible for coordinating and facilitating all aspects of User Functional Testing (UFT). UFT shall be performed by the customer. Customer may require assistance in getting testers set up with test accounts and access to the software to be tested. The completion of User Functional Testing will conclude with the customer signing the Customer Acceptance Form that is anAppendixtothe AcceptanceCriteriaPlan.

1. Ensure each UFT tester test the code using approved Test Cases and Test Scripts and that each test is passed or failed according to the documented pass/failcriteria.
2. Ensure UFT testers have access to the test account to complete testing.
3. EnsuresetupoftestdataiscompletedpriortoUFT.
4. Ensure all required setup or installation instructions are provided to the test users.
5. Support test users in trouble shooting installation and/or access issues.
6. Collect and analyze UFT test results and correct any Severity 1 or 2

Page 29 of 65

VA118-15-F-0663

defects resulting from UFT per the Test Evaluation definition. 7. Ensure any Severity 1 or 2 Defects have related RTC tasks opened,

correlated and assigned.

Deliverables:

1. UFT Test Cases and Test Scripts and Results
2. Signed Customer Acceptance Form

5.4.5 Operational Readiness (OR)

Enterprise Systems Engineering (ESE) Enterprise Testing Service (ETS) may require any of the following test to be performed by their testing group: Requirements Validation Testing, Performance Testing, Integration/Interoperability Testing, Work Product Review (WPR), Test Observation and Validation, Capacity Planning, and Patient Safety Issue (PSI) Testing. The contractor will be alerted to any of these planned tests through the recommendations in the RATSR. The contractor shall:

1. Provide ESE ETS any documentation and software builds required for ESE ETS to complete testing.
2. Track and incorporate ESE ETS test schedules into the Project Schedule as a dependency.
3. Identify and track risks associated with testing related dependencies.
4. Report as “Yellow” or “Red” any testing dependencies that impact  product delivery.

5.4.6 Initial Operating Capability (IOC) Testing

The Contractor shall be responsible for coordinating and facilitating all aspects of IOC Testing. Prior to starting Initial Operating Capability (IOC) Testing, the IOC Entry Request must be completed and submitted to obtain IOC Entry approval from VHA Release Management and. Once these prerequisites have been met, the IOC test sites can install and use the developed solution in their production account for the established timeframe determined during Testing Planning. For this phase of testing, the contractor shall:

1. Complete and submit the IOC Entry Request and ensure all required documentation for the request is complete and available for review.
2. Respond to any questions from the VHA Release Management in support of the IOC Entry Process.
3. Complete any subsequent requirements from VHA Release Management in order to obtain IOC Entry, should they be required.
4. EnsureVistAcodeisprovidedtotestsitesviaFORUM.
5. Ensure all other required setup or installation instructions are provided to the  test sites.
6. Support test sites in trouble shooting installation, setup and use of the solution  for the IOC timeframe.
7. ProvideSQAtesteddefectfixesforSeveritylevel1and2defects

Page 30 of 65

VA118-15-F-0663

discovered during the IOC timeframe. 8. Document defects discovered during IOC in a defect log. 9. Obtain test site concurrence statements at the end of IOC testing. 10.Complete and submit IOC Exit Summary, IOC Site Evaluation Defect Log

and Concurrence Statement to the VHA Release Management Board for approval to Exit IOC.

Deliverables:

5.5

A. IOC Entry Request and Exit Summary B. IOC Site Evaluation Defect Log and Concurrence Statement

Introduction to VistA Intake Program

Following successful IOC testing, the Contractor shall update and finalize all documentation consisting of software code materials, manuals, user guides, and release notes in accordance with PMAS and ProPath. All products shall be delivered to the OneVA Pharmacy COR for acceptance.

The Contractor shall coordinate with the PM to ensure all documentation is provided to the VistA Intake Program (VIP) for review. The Contractor shall attend VIP Technical Review Board (TRB) meetings and VIP Governance Board meetings if/as necessary to present the completed product for consideration.

The Contractor shall conduct lessons learned meetings during and after each Technical Review Board (TRB) meeting and deliver Lesson Learned Reports to document items that can be improved upon and to document issues that need additionalconsideration. UponcompletionoftheTRBdecision,theContractor shall deliver an Implementation Report summarizing the activities performed. If any discrepancies are found, the Contractor shall be responsible for resolve all defects that are discovered post-deployment until resolution until VA Product Support assumes ownership of the application, which is typically thirty (30) days after the completion of the post-completion of the installation window (usually 90 days). Period sites are provided to get the solution installed, provided no defects are identified. The timeliness of defect resolution by the Contractor shall be in accordance with established VA Health Product Support (HPS) timeframes based upon the severity of the defect.

Deliverables: A. Lesson Learned Reports B. Implementation Report

6.1 GENERAL REQUIREMENTS

Page 31 of 65

VA118-15-F-0663

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design(ASD)hasoverall responsibilityfortheOne-VATRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs\_design\_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determinedbythedesignandintegrationpatterns. Directauthenticationata minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M- 05- 24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05- 24.pdf), M-11-11

(http://www.white house.go v/sites/defa ult/files/omb/me moranda/2011/m11 - 11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp- content/uploads/downloads/2012/09/Transition- to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance

            

Page 32 of 65

VA118-15-F-0663

with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va .gov/docume ntlistpub lic.aspx?Node ID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.white house.go v/sites/defa ult/files/omb/assets/o mb/memora nda/fy2008/m0 8- 05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.white house.go v/sites/defa ult/files/omb/assets/o mb/memora nda/fy2008/m0 8- 23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0

https://www.fedramp.go v/files /2015/04/TIC\_Ref\_Arc h\_ v2 -0\_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA’s current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver newcapabilitiesforbusinesssponsorstotestandacceptfunctionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better

         

Page 33 of 65

VA118-15-F-0663

empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and modified templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referencedinSectionDofthe contract.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Page 34 of 65

VA118-15-F-0663

|  |  |
| --- | --- |
|  | neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree. |

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

Position Sensitivity and Background Investigation Requirements by Task



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task Number | Tier1 / Low / NACI | | | Tier 2 / Moderate / MBI | | | Tier 4 / High / BI | | |
| 5.1 |  |  |  |  |  |  |  |  |  |
| 5.2 |  |  |  |  |  |  |  |  |  |
| 5.3 |  |  |  |  |  |  |  |  |  |
| 5.4 |  |  |  |  |  |  |  |  |  |

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS Contractor Responsibilities:

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
2. The Contractor shall bear the expense of obtaining background investigations.
3. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath modified template. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification

Page 35 of 65

VA118-15-F-0663

completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

1. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
2. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
   * 1)  For a Tier 1/Low Risk designation: a) OF-306  b) DVA Memorandum – Electronic Fingerprints
   * 2)  For Tier 2/Moderate or Tier 4/High Risk designation:  a) OF-306 b) VAForm0710 c) DVA Memorandum – Electronic Fingerprints
3. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
4. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
5. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
6. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management  (OPM).

Page 36 of 65

VA118-15-F-0663

1. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
2. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
3. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directedinSectionBofthesolicitation/contract. Acceptableelectronicmediainclude: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

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

|  |  |  |
| --- | --- | --- |
| Performance Objective | Performance Standard | Acceptable Performance Levels |
| A. Technical Needs | 1. Shows understanding of requirements 2. Efficientandeffectivein meeting requirements 3. Meetstechnicalneedsand mission requirements 4. Offersquality services/products | Satisfactory or higher |

Page 37 of 65

VA118-15-F-0663

|  |  |  |
| --- | --- | --- |
| B. Project Milestones and Schedule | 1. Quickresponsecapability 2. Productscompleted,  reviewed, delivered in  timely manner 3. Notifies customer in advance of potential problems | Satisfactory or higher |
| C. Project Staffing | 1. Currencyofexpertise 2. Personnelpossess  necessary knowledge, skills and abilities to perform tasks | Satisfactory or higher |
| D. Value Added | 1. Provided valuable service to Government  2. Services/products delivered were of desired quality | Satisfactory or higher |

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.5 FACILITY/RESOURCE PROVISIONS

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

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

Page 38 of 65

VA118-15-F-0663

Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath,

Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government- provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP’s) and Authority to Operate (ATO)’s for all systems/LAN’s accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED Additional VA Requirements, Consolidated and ADDENDUM B - VA Information And Information System Security/Privacy Language.

6.6 GOVERNMENT FURNISHED PROPERTY

Not Applicable

6.7 SHIPMENT OF DELIVERABLES OR EQUIPMENT

Not Applicable

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

Contractors shall coordinate deliveries with Site POCs before shipment of hardware to ensure sites have adequate storage space. All shipments, either single or multiple container deliveries, will bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (i.e. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

 

Page 39 of 65

VA118-15-F-0663 Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: 116-S56584\_ (i.e., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED A1.0 Cyber and Information Security Requirements for VA IT Services

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

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

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

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

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan

  

Page 40 of 65

VA118-15-F-0663

and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VAInternetandIntranetStandards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor’s work includes managing, maintaining, establishing and presenting information on VA’s Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

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

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

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

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

A3.1. Section508–ElectronicandInformationTechnology(EIT)Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A

   

Page 41 of 65

VA118-15-F-0663

printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

A3.2. EquivalentFacilitation

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

A3.3. Compatibility with Assistive Technology

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

A3.4. AcceptanceandAcceptanceTesting

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

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

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

        

Page 42 of 65

VA118-15-F-0663

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possessionofweaponsisprohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to  perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials

Page 43 of 65

VA118-15-F-0663

pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.

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

Page 44 of 65

VA118-15-F-0663

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

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” dated October 5, 2009; Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” dated January 24, 2007; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere .ene rg y.go v/femp/requireme nts/laws\_a nd\_req uireme nts /ene rg y\_star\_and\_femp\_designated\_products\_procurement\_requirements .The Contractor shall use the low standby power products specified at  http://energy.go v/eere/ femp/ low -sta ndb y-powe r-prod ucts .
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered product.

    

Page 45 of 65

VA118-15-F-0663

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

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

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

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

Page 46 of 65

VA118-15-F-0663

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

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

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

Page 47 of 65

VA118-15-F-0663

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the

Page 48 of 65

VA118-15-F-0663

Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

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

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

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

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

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

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding- Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Page 49 of 65

VA118-15-F-0663

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

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

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

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

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

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

Page 50 of 65

VA118-15-F-0663

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

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

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

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

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

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

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

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the

Page 51 of 65

VA118-15-F-0663 availability of the system). Such issues shall be remediated as quickly as is practical,

based upon the severity of the incident.

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

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

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor’s security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor’s systems in accordance with VA Handbook 6500.3, Certification and Accreditation and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

Page 52 of 65

VA118-15-F-0663

d. The Contractor/Subcontractor’s system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

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

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

Page 53 of 65

VA118-15-F-0663

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

* 1)  Vendor must accept the system without the drive;
* 2)  VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
* 3)  VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
* 4)  Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

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

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

Page 54 of 65

1) 2)

3)

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

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

Number of individuals affected or potentially affected;

VA118-15-F-0663

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

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

Page 55 of 65

B8.

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

SECURITY CONTROLS COMPLIANCE TESTING

VA118-15-F-0663

* 4)  Names of individuals or groups affected or potentially affected;
* 5)  Ease of logical data access to the lost, stolen or improperly accessed data in

light of the degree of protection for the data, e.g., unencrypted, plain text;

* 6)  Amount of time the data has been out of VA control;
* 7)  The likelihood that the sensitive personal information will or has been

compromised (made accessible to and usable by unauthorized persons);

* 8)  Known misuses of data containing sensitive personal information, if any;
* 9)  Assessment of the potential harm to the affected individuals;
* 10)  Data breach analysis as outlined in 6500.2 Handbook, Management of

Security and Privacy Incidents, as appropriate; and

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

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

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

Page 56 of 65

VA118-15-F-0663

(to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

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

1) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix D relating to access to VA information and information systems.

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

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

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

VA Program Manager:

Name: Joshua Patterson Address: 3773 Cherry Creek North Drive

Denver, CO 80209 Voice: 303.809.7870

Email: joshua.patterson@ va.go v

Contracting Officer’s Representative:

Name: Joshua Patterson Address: 3773 Cherry Creek North Drive

Denver, CO 80209 Voice: 303.809.7870

Email: joshua.patterson@ va.go v Contracting Officer:

   

Page 57 of 65

Name: Mark R. Junda Address: Department of Veterans Affairs

Technology Acquisition Center 23 Christopher Way Eatontown, New Jersey 07724

Voice: 732-795-1019 Email: Mark.Junda@va.gov

Contract Specialist:

Name: Amy Schmalzigan Address: Department of Veterans Affairs

Technology Acquisition Center 23 Christopher Way Eatontown, New Jersey 07724

Voice: 732-795-1121 Email: Amy.Schmalzigan@va .go v

VA118-15-F-0663

 

Page 58 of 65

FAR Number 52.204-4

52.227-1 52.227-2

Title

PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER

AUTHORIZATION AND CONSENT NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT

Date

MAY 2011

DEC 2007 DEC 2007

VA118-15-F-0663

SECTION C - CONTRACT CLAUSES

C.1 FEDERALSUPPLYSCHEDULE(FSS)REQUESTFORQUOTE(RFQ) INTRODUCTORY LANGUAGE

The terms and conditions of the contractor's FSS contract (including any contract modifications) apply to all Blanket Purchase Agreements (BPA) and task or delivery orders issued under the contract as a result of this RFQ. When a lower price has been established, or when the delivery terms, FOB terms, or ordering requirements have been modified by the BPA or task/delivery order, those modified terms will apply to all purchases made pursuant to it and take precedence over the FSS contract. Any unique terms and conditions of a BPA or order issued under the contract that are not a part of the applicable FSS contract will govern. In the event of an inconsistency between the terms and conditions of a BPA or task/delivery order and the Contractor's FSS terms, other than those identified above, the terms of the FSS contract will take precedence.

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

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

   

C.3 52.203-99 PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION) (FEB 2015)

* (a)  The Contractor shall not require employees or contractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
* (b)  The contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this clause are no longer in effect.

Page 59 of 65

VA118-15-F-0663

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d)(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(2) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

(End of Clause)

C.4 52.227-3 PATENT INDEMNITY (APR 1984) ALTERNATE III (JUL 1995)

(a) The Contractor shall indemnify the Government and its officers, agents, and employees against liability, including costs, for infringement of any United States patent (except a patent issued upon an application that is now or may hereafter be withheld from issue pursuant to a Secrecy Order under 35 U.S.C. 181) arising out of the manufacture or delivery of supplies, the performance of services, or the construction, alteration, modification, or repair of real property (hereinafter referred to as "construction work") under this contract, or out of the use or disposal by or for the account of the Government of such supplies or construction work.

(b) This indemnity shall not apply unless the Contractor shall have been informed as soon as practicable by the Government of the suit or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. Further, this indemnity shall not apply to (1) an infringement resulting from compliance with specific written instructions of the Contracting Officer directing a change in the supplies to be delivered or in the materials or equipment to be used, or directing a manner of performance of the contract not normally used by the Contractor, (2) an infringement resulting from addition to or change in supplies or components furnished or construction work performed that was made subsequent to delivery or performance, or (3) a claimed infringement that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

(c) As to subcontracts at any tier for communication service, this clause shall apply only to individual communication service authorizations over $25,000 issued under this contract and covering those communications services and facilities (1) that are or have been sold or offered for sale by the Contractor to the public, (2) that can be provided over commercially available equipment, or (3) that involve relatively minor modifications.

Page 60 of 65

VA118-15-F-0663

(End of Clause)

C.5 52.227-16 ADDITIONAL DATA REQUIREMENTS (JUN 1987)

(a) In addition to the data (as defined in the clause at 52.227-14, Rights in Data— General clause or other equivalent included in this contract) specified elsewhere in this contract to be delivered, the Contracting Officer may, at any time during contract performance or within a period of 3 years after acceptance of all items to be delivered under this contract, order any data first produced or specifically used in the performance of this contract.

(b) The Rights in Data—General clause or other equivalent included in this contract is applicable to all data ordered under this Additional Data Requirements clause. Nothing contained in this clause shall require the Contractor to deliver any data the withholding of which is authorized by the Rights in Data—General or other equivalent clause of this contract, or data which are specifically identified in this contract as not subject to this clause.

(c) When data are to be delivered under this clause, the Contractor will be compensated for converting the data into the prescribed form, for reproduction, and for delivery.

(d) The Contracting Officer may release the Contractor from the requirements of this clause for specifically identified data items at any time during the 3-year period set forth in paragraph (a) of this clause.

(End of Clause)

C.6 52.227-19 COMMERCIALCOMPUTERSOFTWARELICENSE(DEC2007)

(a) Notwithstanding any contrary provisions contained in the Contractor's standard commercial license or lease agreement, the Contractor agrees that the Government will have the rights that are set forth in paragraph (b) of this clause to use, duplicate or disclose any commercial computer software delivered under this contract. The terms and provisions of this contract shall comply with Federal laws and the Federal Acquisition Regulation.

(b)(1) The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b)(2) of this clause or as expressly stated otherwise in this contract.

(2) The commercial computer software may be—

Page 61 of 65

VA118-15-F-0663

(i) Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation to which the computer(s) may be transferred;

(ii) Used or copied for use with a backup computer if any computer for which it was acquired is inoperative;

(iii) Reproduced for safekeeping (archives) or backup purposes;

(iv) Modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, commercial computer software shall be subject to same restrictions set forth in this contract;

(v) Disclosed to and reproduced for use by support service Contractors or their subcontractors, subject to the same restrictions set forth in this contract; and

(vi) Used or copied for use with a replacement computer.

(3) If the commercial computer software is otherwise available without disclosure restrictions, the Contractor licenses it to the Government without disclosure restrictions.

(c) The Contractor shall affix a notice substantially as follows to any commercial computer software delivered under this contract:

Notice—Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Government Contract No. \_ GS-35F-0662S VA118-15-F-0663 \_\_.

(End of Clause)

C.7 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

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

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or

Page 62 of 65

VA118-15-F-0663

agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

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

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

(End of Clause)

C.8 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

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

(End of Clause)

C.9 VAAR 852.203-71 DISPLAY OF DEPARTMENT OF VETERAN AFFAIRS HOTLINE POSTER (DEC 1992)

(a) Except as provided in paragraph (c) below, the Contractor shall display prominently, in common work areas within business segments performing work under VA contracts, Department of Veterans Affairs Hotline posters prepared by the VA Office of Inspector General.

(b) Department of Veterans Affairs Hotline posters may be obtained from the VA Office of Inspector General (53E), P.O. Box 34647, Washington, DC 20043-4647.

(c) The Contractor need not comply with paragraph (a) above if the Contractor has established a mechanism, such as a hotline, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.

(End of Clause)

C.10 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

(a) Definitions. As used in this clause— (1) Contract financing payment has the meaning given in FAR 32.001. (2) Designated agency office has the meaning given in 5 CFR 1315.2(m).

Page 63 of 65

VA118-15-F-0663

(3) Electronic form means an automated system transmitting information electronically according to the

Accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) Invoice payment has the meaning given in FAR 32.001. (5) Payment request means any request for contract financing payment or invoice

payment submitted by the contractor under this contract.

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

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

(1) VA’s Electronic Invoice Presentment and Payment System. (See Web site at http://www.fsc.va.gov /einvoice.asp.)

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI). The X12 EDI Web site (http://www.x12.org) includes additional information on EDI 810 and 811 formats.

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

(e) Exceptions. If, based on one of the circumstances below, the contracting officer directs that payment requests be made by mail, the contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for:

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

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

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

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

Page 64 of 65

VA118-15-F-0663

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

(End of Clause)

C.11 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

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

(End of Clause)

Page 65 of 65