|  |
| --- |
| VeteransAffairs-Seal.JPG |

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

**VETERANS BENEFITS AGENCY**

**LOAN GUARANTY (LGY) PROGRAM**

**VETERANS AFFAIRS**

**LOAN ELECTRONIC REPORTING INTERFACE (VALERI)**

**Date: 1/7/2013**

**TAC-13-06554**

**PWS Version Number: 1.5.3**

Contents

[1.0 BACKGROUND 4](#_Toc376945728)

[2.0 APPLICABLE DOCUMENTS 5](#_Toc376945729)

[3.0 SCOPE OF WORK 7](#_Toc376945730)

[4.0 PERFORMANCE DETAILS 8](#_Toc376945731)

[4.1 PERFORMANCE PERIOD 8](#_Toc376945732)

[4.2 PLACE OF PERFORMANCE 8](#_Toc376945733)

[4.3 TRAVEL 8](#_Toc376945734)

[5.0 SPECIFIC TASKS AND DELIVERABLES 9](#_Toc376945735)

[5.1 PROJECT MANAGEMENT 10](#_Toc376945736)

[5.1.1 PROJECT MANAGEMENT PLAN 11](#_Toc376945737)

[5.1.2 MONTHLY STATUS REPORTS (MSR) 12](#_Toc376945738)

[5.1.3 QUARTERLY MANAGEMENT BRIEFING 12](#_Toc376945739)

[5.2 VALERI SERVICES 12](#_Toc376945740)

[5.2.1 INTERFACES 15](#_Toc376945741)

[5.2.1.1 Security Deliverables 15](#_Toc376945742)

[5.2.1.2 MORTGAGE SERVICER PERSONNEL INTERFACE [CURRENTLY KNOWN AS SERVICER WEB PORTAL (SWP)] 15](#_Toc376945744)

[5.2.1.3 AUTOMATED MORTGAGE SERVICER INTERFACE (CURRENTLY KNOWN AS DIRECT CONNECT) 16](#_Toc376945745)

[5.2.1.4 VA PERSONNEL USER INTERFACE 16](#_Toc376945746)

[5.2.1.5 VA AUTOMATED SYSTEMS INTERFACE 17](#_Toc376945747)

[5.2.2 REPORTING 17](#_Toc376945748)

[5.2.3 SERVICER ANALYSIS 18](#_Toc376945749)

[5.2.4 TESTING 19](#_Toc376945750)

[5.2.4.1 TEST PLAN 19](#_Toc376945751)

[5.2.4.2 TEST SCENARIOS AND SCRIPTS 19](#_Toc376945752)

[5.2.5 LIMITED USE PILOT OF PRODUCTION VALERI SOLUTION 20](#_Toc376945753)

[5.2.6 “ALL USER” IMPLEMENTATION 20](#_Toc376945754)

[5.2.7 DISASTER RECOVERY (DR) 20](#_Toc376945755)

[5.2.8 USER TRAINING 21](#_Toc376945756)

[5.3 OPERATE, MAINTAIN AND ENHANCE VALERI SOLUTION 22](#_Toc376945757)

[5.3.1 ON-GOING TESTING 23](#_Toc376945758)

[5.3.2 CUSTOMER SERVICE/HELP DESK SUPPORT/TICKET TRACKING 23](#_Toc376945759)

[5.4 EXIT TRANSITION 24](#_Toc376945760)

[5.5 OPTION PERIODS 25](#_Toc376945761)

[5.5.1 OPTION PERIOD 1: 25](#_Toc376945762)

[5.5.2 OPTION PERIOD 2: 25](#_Toc376945763)

[5.5.3 OPTION PERIOD 3: 25](#_Toc376945764)

[5.5.4 OPTION PERIOD 4: 25](#_Toc376945765)

[6.0 GENERAL REQUIREMENTS 25](#_Toc376945766)

[6.1 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 25](#_Toc376945767)

[6.1.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 25](#_Toc376945768)

[6.2 METHOD AND DISTRIBUTION OF DELIVERABLES 29](#_Toc376945769)

[6.3 PERFORMANCE METRICS 29](#_Toc376945770)

[6.4 FACILITY/RESOURCE PROVISIONS 31](#_Toc376945771)

[6.5 GOVERNMENT FURNISHED PROPERTY 31](#_Toc376945772)

[6.6 RIGHTS IN DATA 31](#_Toc376945773)

[6.7 ACRONYM LIST 32](#_Toc376945774)

[6.8 LIST OF ATTACHMENTS 34](#_Toc376945775)

[ADDENDUM A 36](#_Toc376945776)

[ADDENDUM B 41](#_Toc376945777)

# BACKGROUND

The Department of Veterans Affairs (VA) Loan Guaranty (LGY) Program provides home loan benefits to eligible Veterans obtaining mortgage loans through private lenders by guaranteeing a portion of the loan against default. This allows Veterans to obtain mortgage loans at competitive rates with little or no down payment. When a default occurs on these guaranteed loans, Veterans receive help in retaining their homes and minimizing their financial losses through primary servicing performed by their servicers and servicing by exception performed by VA. Veterans Affairs Loan Electronic Reporting Interface (VALERI) was conceptualized to enable Loan Administration (LA) to improve services to Veterans, improve oversight capability over VA loan servicers, and to reduce the cost to the Government for defaulted loans.

VALERI supports VA and LGY mission in helping Veterans and their families retain their homes.

The current VALERI is a web-enabled rules-based solution, designed to improve VA’s oversight capability and to reduce the cost to the Government for the servicing and liquidation of VA-guaranteed loans. It provides an interface between VA and the mortgage servicing community, allowing mortgage servicers to report significant event updates to VA focusing on default, loss mitigation, foreclosure, and claim payments. The current VALERI provides both a web-interface and an integration component to allow automated loading of updates from VA mortgage servicers. The web-interface allows VAs technicians to manage VA loans and evaluate servicer performance, allowing VA to intervene on the Veteran’s behalf, when necessary. Implementation of VALERI began February 20, 2008. Since November 2008, all servicers and all VA-guaranteed loans have been managed through the current VALERI environment. Currently, VALERI assists VA in managing over 1.7 million active and 1.5 million inactive VA loans (inactive loans are defined as 425 calendar days following the termination of a VA loan). By Fiscal Year (FY) 2019, VA anticipates managing 2.6 million active and 10 million inactive loans.

VALERI is able to accomplish VA’s mission of providing improved service to Veterans by:

* Providing Veterans assistance earlier in the default;
* Maximizing loss mitigation;
* Standardizing organizational structure;
* Providing total case management;
* Conducting post-audits of servicer actions to ensure compliance;
* Offering detailed reports on performance data;
* Offering standardized and recurring employee training; and
* Providing data on all outstanding VA-guaranteed loans.

In May of 2009, VA awarded a sole source Task Order (TO) to Lender Processing Services (LPS) to perform overall project management and progress reporting as well as all technical requirements of developing, implementing, and training personnel on the VALERI solution.

LPS developed and owns the source code for the existing VALERI solution, which will only be available to that company. VA owns the historical loan data within VALERI. VALERI is a VA acronym and VA intends to publicly use the VALERI name in this solicitation and as well as in future solicitations.

# APPLICABLE DOCUMENTS

This solicitation incorporates the following documents by reference, with the same force and effect as if they were given in full text. The Contractor shall comply with these documents in performance of this PWS:

1. Privacy Act, 5 United States Code (U.S.C.) §552a, which can be found at: http://www.justice.gov/opcl/privstat.htm;
2. VA Directive 6500, Information Security Program (VA Handbook 6500.6, Contract Security, which is available at: http://www1.va.gov/vapubs;
3. Veterans Health Administration (VHA) Directive 0710 (Implementation Handbook 0710.01, which are available at: http://www1.va.gov/vapubs and <http://www1.va.gov/vhapublications/index.cfm>);
4. Veterans Affairs Acquisition Regulation (VAAR)-852.273-75: Security Requirements for Unclassified Information Technology (IT) Resources (Interim-October 2008), http://www.ahcancal.org/facility\_operations/hit/Documents/ITrequirements.pdf;
5. Federal Information Security Management Act (FISMA),
6. Appendix III of Office of Management and Budget (OMB) Circular A-130, <http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii>,
7. and guidance and standards, available from the Department of Commerce’s National Institute of Standards and Technology (NIST);
8. Rights in Data - General, Federal Acquisition Regulation (FAR) 52.227-14(d)(1), https://www.acquisition.gov/far/current/html/Subpart%2027\_4.html;
9. VA Directive 6300, Records and Information Management (VA Handbook 6300.1 Records Management Procedure, and all applicable VA Records Control Schedules), http://www1.va.gov/vapubs/viewPublication.asp?Pub\_ID=475&FType=2;
10. VA Information and Information System Security/Privacy Requirements for IT Contracts, which is available at: <http://www.iprm.oit.va.gov>**;**
11. VA Directive 0730, Section 6 (Physical Security), http://www.va.gov/vapubs/viewPublication.asp?Pub\_ID=94&FType=2;
12. VA Memorandum: IT Oversight & Compliance Information Physical Security Assessments, October 24, 2007;
13. VA Directive 0710, September 10, 2004, which is available at: <http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FType=2>;
14. Rights in Data and Copyrights, FAR 27.401 Definitions, https://www.acquisition.gov/far/current/html/Subpart%2027\_4.html;
15. VA Regulations 38 Code of Federal Regulations (CFR) 4300 Series <http://www.benefits.va.gov/homeloans/VALERI.asp>;
16. Information related to VA’s Home Loan program, <http://www.benefits.va.gov/homeloans>;
17. Americans with Disabilities Act (ADA) Compliance (Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended), <http://www.access-board.gov/sec508/standards.htm>;
18. Servicing System Interface Document, Attachment A, *(*<http://www.benefits.va.gov/homeloans/VALERI.asp>)
19. VALERI Technician Guide, Attachment B;
20. LGY Business Rules, Attachment C;
21. VALERI Reporting Library, Attachment D;
22. Software Requirements Specifications (SRS), Attachment E;
23. Process and steps for all active processes, Attachment F; and
24. VALERI Servicer Guide, <http://www.benefits.va.gov/homeloans/valeri.asp>, **under Document Library for Servicers Live in VALERI (VA Servicer Guide)**;
25. Project Management Institute’s (PMI™) Project Management Body of Knowledge (PMBOK);
26. VA Office of Information and Technology (OIT) Project Management Guide.

# SCOPE OF WORK

The scope of this effort is to acquire services consistent with the existing VALERI solution as well as the requirements stated in this Performance Work Statement (PWS). The solution shall provide the following services:

* Existing integrations with mortgage servicing systems and mortgage servicing bureaus to support daily, or more frequent updates, of all VA-guaranteed loans, the storage of these updates and any historical data associated with these loans;
* Interface with VA systems to support data exchange, financial transactions with the mortgage servicers, etc.;
* Maintenance and continuous enhancement of a web-enabled, rule based and role-specific Graphical User Interface (GUI) for the servicing community and VA to support total case management.
* Reporting and analysis of the performance of the VA portfolio, the services provided, etc.
* Training and Helpdesk support services for all VALERI users, including VA staff and mortgage industry participants.
* Program/project management in support of all activities associated with this PWS.

The services shall ensure all loss mitigation, supplemental servicing, claims processing, and foreclosure-related activities continue, uninterrupted at all times. The services shall also include all transition tasks including the start-up of newly provided services and the sunset/exit transition of services to any newly identified providers. The selected Contractor shall provide all resources necessary to accomplish the requirements described in this PWS, except as otherwise specified.

The detailed requirements are identified in four (4) main functional areas shown in the table below. Detailed descriptions of those areas are available in Section 5.0 “Tasks and Deliverables.”

| **FUNCTIONAL AREA** | **PWS SECTION** |
| --- | --- |
| Project Management | 5.1 |
| VALERI Services | 5.2 |
| Operate, Maintain and Enhance VALERI Solution | 5.3 |
| Exit Transition | 5.4 |

The Contractor shall provide all resources necessary to accomplish the requirements described in this PWS.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The period of performance shall be one (1) partial year base period with four (4) 12-month option periods and one partial year option period, for a total of 5 years. All work identified in this PWS shall be performed at the Contractor’s facility(s).

## PLACE OF PERFORMANCE

## TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings through the period of performance.  Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government. International travel will not be required.

VA anticipates no more than four (4), week-long (including travel days), meetings per year to VA’s Central Office (VACO) located in Washington, District of Columbia (D.C.) to review program progress, and discuss contractual issues.

VA anticipates no more than six (6), week-long (including travel days), meetings per year to mortgage servicer sites or industry events to conduct training, gather program and solution feedback, *etc*.

VA anticipates no more than four (4) meetings, week-long (including travel days), per year to VA Regional Loan Centers (RLCs) or locations to conduct training, gather program and solution feedback, *etc.*, located in:

* Atlanta, Georgia
* Austin, Texas
* Cleveland, Ohio
* Denver, Colorado
* Houston, Texas
* Phoenix, Arizona
* Roanoke, Virginia
* St. Paul, Minnesota
* St. Petersburg, Florida

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall provide all tasks and deliverables described within this document. All deliverables shall be submitted to the Contracting Officer (CO) and Contracting Officer’s Representative (COR), in accordance with PWS, Schedule of Deliverables, and shall meet the standards set forth in the Quality Assurance Surveillance Plan (QASP). The COR, or other designated representative(s) will discuss and come to an agreement with the Contractor on the specific contents of the deliverables identified in this PWS. Inspection and acceptance of all work performance, reports and other deliverables under this contract shall be performed by the COR. Unless otherwise stipulated, written deliverables shall be phrased in plain English. Statistical and other technical terminology shall not be used without providing a glossary of terms (refer to Section 6.7).

The services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a Successor, either the Government or another Contractor, may continue them. Upon contract award, the Contractor shall begin preparation to ensure full functionality of the solution on the day after the current contract expires. Note: The current contract will expire as of June 30, 2014, by which time the Contractor’s solution must be fully designed, developed, tested, and deployed. The Contractor’s Project Schedule shall reflect this. The Contractor shall ensure seamless transition to the services specified in this PWS on July 1, 2014. As part of the transition, the Contractor shall provide the following:

1. Project Management;
2. Transition to the new VALERI environment, including migration of that data to the new VALERI environment;
3. Implementation, including pilot, and deployment activities;
4. Training of all users; and
5. Coordination with VA, the current solution provider and successors.

More information on the requirements for this PWS is provided below.

The following sections describe the underlying technical and management constraints and considerations that support the VA’s objectives. There are four (4) functional areas of tasks that the Contractor shall provide under this PWS: Project Management, VALERI Services, Operate, Maintain and Enhance VALERI Solution, and Exit Transition.

The Contractor shall use best commercial practices for formatting deliverables under this contract. Additionally, electronic copies shall be delivered via email attachment in Microsoft (MS) Office Suite or Adobe formats (refer to Section 6.2). The Contractor shall label each email with the Contract Number and Project Title in the subject line. The Contractor shall maintain a MS SharePoint site or similar technology accessible by VA where it shall store all applicable deliverables associated with this PWS. All documentation including systems requirements, training materials, on-line resources, user guide, *etc.*, shall be continuously updated immediately following changes to the solution. Notification of the addition of new materials and updates shall be provided to the COR via email. The Contractor shall update and retain all VALERI-related documentation including business requirements, technical requirements, use cases, and so forth throughout the life of this contract.

## PROJECT MANAGEMENT

The Contractor shall provide comprehensive Project Management under this contract. The Project Management Plan, in compliance with Project Management Institute’s (PMI™) Project Management Body of Knowledge (PMBOK), shall include the management and oversight of all activities performed by Contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. A key personnel for this effort is the Project Manager. The Contractor shall identify a Project Manager, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this contract.

The Contractor shall schedule and coordinate a Project Kick-Off Meeting within five (5) business days of contract award, at the location approved by the Government, but most likely in the Washington, D.C. area. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the contract. The meeting will provide the opportunity to discuss all aspects of the PWS. The Contractor shall participate in monthly/quarterly status meetings to ensure success of the project and shall prepare monthly/quarterly status and progress reports until such time that the CO/COR/Authorized Designee elects to modify this schedule in writing.  The Contractor shall provide meeting minutes for the monthly/quarterly status meetings to the COR with a copy to the CO within 48 hours of the meeting. The Contractor shall keep in communication with the CO/COR accordingly so that issues that arise are transparent to both parties and outstanding issues are not escalated.

The Contractor shall ensure audits and assessments do not have substantive findings (material weaknesses or significant deficiencies). The Contractor shall provide VA with a written response to all non-substantive findings within one (1) month and resolution within two (2) months from the date of notification. The Contractor shall provide VA with a written response to all substantive findings within two (2) weeks and resolution within four (4) weeks from the date of notification. The Contractor shall generate, collect, distribute, store, retrieve, and dispose of project information. VA will retain all rights to information, data, deliverables, *etc.*, developed in support in this PWS with the exception of the COTS source code developed by the Contractor through the project included in the deliverables and otherwise.

In addition, the Contractor shall:

1. Provide VA with an updated list of phone numbers, addresses, email addresses for key personnel that regularly interact with VA;
2. Ensure all documents are tracked using dated version control.

**Deliverables:**

1. Project Kickoff Meeting Minutes
2. Quarterly Status Meeting Minutes
3. Written Responses to all non-substantive findings
4. Written Responses to all substantive findings

### PROJECT MANAGEMENT PLAN

The Contractor shall provide a detailed Project Management Plan (PMP), in compliance with Project Management professional standards, specifically Project Management Institute’s (PMI™) Project Management Body of Knowledge (PMBOK) [e.g.; Communications Management Plan, Quality Control Plan (QCP), Human Resources Management Plan, Risk Management Plan, Work Breakdown Structure (WBS), Schedule Management Plan, *etc*.,]; and the VA Office of Information and Technology (OIT) Project Management Guide which will cover all work to be completed within this contract and shall include a project schedule that is updated regularly to reflect any changes. The PMP shall be kept current throughout the life of the project and shall be used in part to track progress.  An updated PMP reflecting those changes shall be delivered during the Monthly/Quarterly briefings on the 3rd business day of every month. Work shall not commence until the VA PM approves the PMP.

Included with the PMP, the Contractor shall:

1. Explain how the Contractor shall encourage high quality performance of both employees and subcontractors;
2. Ensure the separation of duties between operations and audit/oversight staff;
3. Proactively recommend and implement process and technology improvements that positively impact operations on the requirements;
4. Address tasks within this PWS to include measurable outcomes and definitions of success;
5. Contain officer certifications, authorized signers, as well as plans to mitigate known risks; and
6. Address critical aspects of the Contractor’s offering to VA, including known industry issues.

Note: The current contract will expire as of June 30, 2014, by which time the Contractor’s solution must be fully designed, developed, tested, and deployed. The Contractor’s Project Schedule shall reflect this.

**Deliverable:**

1. Detailed PMP and Briefing

### MONTHLY STATUS REPORTS (MSR)

The Contractor shall develop and provide a MSR using MS Office Suite applications, by the third business day of each month via electronic mail to the COR. Each report shall include the following:

1. Activities by task during reporting period to include: on-going activities, new activities, and activities completed; progress to date; and a brief description of the task;
2. Problems/issues and corrective actions taken (issues or concerns and proposed resolutions to address them); and
3. Schedule deviations.

**Deliverable:**

1. MSRs

### QUARTERLY MANAGEMENT BRIEFING

The Contractor shall provide a QSR, due the third business day of each quarter, which describes, at a minimum, the tasks, progress, and accomplishments for the period since the last quarterly briefing.

**Deliverable:**

1. Quarterly Management Briefing

## VALERI SERVICES

The Contractor shall provide services consistent with the existing VALERI solution and in accordance with the PWS, and the following attachments:

1. Attachment A - Servicing System Interface Document
2. Attachment B - VALERI Technician Guide
3. Attachment C - LGY Business Rules
4. Attachment D - VALERI Reporting Library
5. Attachment E - Software Requirements Specifications (SRS)
6. Attachment F - Process And Steps For All Active Processes

The Contractor’s solution which offers the VALERI services shall include existing interfaces with mortgage-servicing systems and mortgage-servicing bureaus that collect loan data on VA-guaranteed loans, interpret that data and drive business workflow for those loans..

The Contractor’s solution shall provide authorized industry and VA personnel with real time, 24/7/365, secured internet, and direct connection access to all production data and records. The service shall be fully operational 99.9% throughout the period of performance. The solution shall be compatible with versions of Internet Explorer (IE) currently supported by Microsoft or used by VA, in addition to browsers commonly used by industry, as defined by VA. The solution shall provide response times acceptable to VA, but no more than .5 second with 1,000 concurrent users. The solution shall be web-based graphical user interface (GUI), capable of supporting more than 10,000 users across nearly 400 different servicing companies, , 3.2 million loans at any given time.

The Contractor’s solution shall be readily capable to scale up to accommodate growth in a manner transparent to VA and its user base. (See Attachment F, SRS Document, Section 2.2 – User Classes and Characteristics.) Currently VALERI maintains 10,247 users, which includes 9,777 servicer users and 470 VA users daily, data exchanges with 391 servicers in the industry, processing over 142 event files daily and maintaining a web portal for the remaining servicers’ use. Currently, VALERI assists VA in managing over 1.7 million active and 1.5 million inactive VA loans (inactive loans are defined as 425 calendar days following the termination of a VA loan). By FY2019, VA anticipates managing 2.6 million active and 9.5 million inactive loans, which will be accommodated by the Contractor’s solution.

The Contractor’s solution shall maintain an electronic interface with three (3) VA systems, or their replacements in the unlikely event they are replaced, processing 12 transaction files daily for VA.

In addition to conducting work on production data for the entire VA-Guaranteed Loan portfolio, the Contractor’s solution shall provide the ability for VALERI users to;

* Conduct user acceptance testing (UAT) in an environment that mirrors production. Test cases used in UAT shall not affect production data.
* Conduct training in an environment that mirrors production. Training cases used for training purposes shall not affect production data.
* Create and manipulate cases used for testing or training, based on fictional scenarios provided by VA or by copying actual production cases, without affecting production data. The ability to copy actual production cases, as stated above, is limited to specifically identified VA employees.

The Contractor’s solutions shall:

1. Ensure that VALERI users shall not be required to provide Personally Identifiable Information (PII) such date of birth, social security number, for access to the solution.
2. Keep records satisfactory to VA pertaining to each loan for the duration of the contract (Records and related documentation are VA’s property).

The Contractor’s solution shall provide data processing that involves updating and maintaining a loan from origination until the loan is paid-in-full or terminated. The solution shall be designed to automate and integrate the critical processes that involve loan servicing, pre-approvals per VA regulation, loss mitigation, foreclosure, claims, appeals, and post audit. These processes shall be managed and maintained by administration tools and code enhancements.

The Government will provide electronic records and data necessary to establish the historical actions taken by or documented by the VA, in relation to specific loans contained within the existing VALERI environment. The Contractor shall be responsible for merging this information with any newly acquired information, on a loan level basis, or otherwise, as it relates to the requirements herein. This imported data shall be available in the production version of the Contractor’s solution at all times.

The Contractor’s solution shall identify and process cases for adequacy of servicing reviews; identify and log regulatory infractions; identify suspicious loss mitigation workouts; identify cases with substantial equity; accept entries of decisions related to loss mitigation recommendations, refund transactions, Bills of Collection (BOCs), incentive payments, acquisition payments and claim payments; and process pre-approvals, appeals and post-audits.

The Contractor’s solution shall receive loan data on a daily basis and compare it to previously submitted data. The solution shall provide the capability to determine if any changes were made to the data and generate appropriate regulatory events based on the VA Business Rules. (This function is currently known as the Event Interpreter.) VA has developed business rules for each event, which shall be examined by the solution via a business rules engine. The solution shall make available the results for VA review. Historically, there has been one (1) large revision to the Business Rules during the four (4) years, which was a one (1)-time correction to a known design flaw. VA anticipates future changes to be minor.

The Contractor’s solution shall monitor and track for regulatory events that initiate data processes for action by VA personnel, which are then assigned to individual workbaskets or work queues. VA has established steps for each process, which are tracked and completed in VALERI, within a required timeframe (refer to Attachment C, VALERI Technician Guide). The Contractor’s solution shall include all functionalities, interfaces, and processes such as Event Interpreter Functionality, Data Processing, Process Creation Functionality, Business Rules, *etc*.

### INTERFACES

The Contractor’s solution shall provide four (4) interfaces to support VA personnel, mortgage servicer personnel, mortgage servicing systems, and VA systems.

### Security Deliverables

### The contractor shall maintain continual compliance and deliver against the requirements set forth in Addendum X in order for any interface connection with VA network or systems to be tested, piloted or used to production.

### MORTGAGE SERVICER PERSONNEL INTERFACE [CURRENTLY KNOWN AS SERVICER WEB PORTAL (SWP)]

The Contractor’s solution shall allow mortgage servicers to login and manually upload or enter loan data into the solution for an individual event on individual loans or upload multiple events on multiple loans at once. Additionally, the mortgage servicer shall be able to view information previously submitted, as well as submit events, including, but not limited to:

1. Claims – Servicers have the option of manually inputting a claim or building an interface to submit automated claims for loans terminated through foreclosure, deed-in-lieu (DIL) of foreclosure, and compromise sale. They shall have the ability to submit supplemental claims and claims for refunded loans. VALERI automatically processes all terminated loan claims electronically when servicers report the Basic Claim event.
2. Appeals – Servicers may appeal a VA decision, including but not limited to on unpaid and paid incentives, claims, claim line items, post audits, acquisitions, regulatory infractions, BOCs, and late claims.
3. Post Audit – The post audit is one (1) of the core processes that enable the VA to monitor servicer performance and adherence to VA policies and regulations, and validate payments. VA post audits consist of a random selection of cases with repayment plans, special forbearances, loan modifications, DILs, compromise sales, and terminated/foreclosed loans, with and without claims and partial releases of security.

### AUTOMATED MORTGAGE SERVICER INTERFACE (CURRENTLY KNOWN AS DIRECT CONNECT)

The Contractor’s solution shall interface with the servicing community (e.g., Servicer Proprietary Systems, Servicer Licensed Mortgage Servicing Systems, Mortgage Servicing Bureaus,) to support automatic detection of regulation-required events from servicer-provided data that is submitted daily. VA has specified a list of 204 fields to be provided by the servicing community in daily extracts (See Attachment B - Servicing System Interface Document Version 10 Final, dated Nov 17, 2008).

### VA PERSONNEL USER INTERFACE

The Contractor’s solution shall provide a customized COTS GUI so that VA personnel can login, review, and complete queued work that is based on events generated by the solution from data submitted by loan servicers. Examples of these processes include, but are not limited to:

* Access case information for current and delinquent loans;
* Conduct adequacy of servicing reviews;
* Assign/reassign cases;
* Manage workbaskets (i.e., work queues,);
* Review and enter case notes;
* Complete loss mitigation actions;
* Provide pre-approval of exception cases;
* Review, approve and certify appeals;
* Review, approve and certify claims;
* Review, approve and certify incentives;
* Review, approve and certify post audits;
* Review substantial equity cases;
* Review early payment default loan;
* Review, approve and certify BOCs;
* Review and approve property conveyances;
* Review and approve Refund Considerations;
* Review returns of custody; and
* Upload documents.

### VA AUTOMATED SYSTEMS INTERFACE

The Contractor’s solution shall maintain VA Automated Systems Interfaces. On a daily basis, VALERI manages the receipt and processing of files from other VA systems and generates files to be sent to those systems. These processes run automatically to ensure each file is processed the day it is received. (For additional details, reference Attachment B, System Interface document) The types of files received and transmitted from/by VA are:

* Loan origination and appraisal information from Web-enabled Loan Guaranty System (WebLGY) and sending information on loan terminations to WebLGY;
* Property management assignments and withdrawals to Centralized Property Tracking System (CPTS), which sends acknowledgments to VALERI; and
* Financial information to and from the VALERI solution via several Financial Management System (FMS) files. The FMS files are processed at time of receipt in VALERI. Several FMS files are also transmitted daily from VALERI to FMS that contain payment transaction and BOC data.

### REPORTING

The Contractor shall provide a flexible reporting capability to allow VA management to analyze operational loan servicing data, the performance of the VA portfolio, financial information, and metrics for VA employees, and servicer performance. (For additional details, see Attachment D – VALERI Reporting Library and Attachment F – SRS (System Requirement Specification).) The solution shall allow authorized VA users to analyze information across several dimensions, in support of all VA loan servicing, loss mitigation, supplemental servicing, and remittance functions. The VALERI data populates the reporting application on a daily basis, at a minimum. The Contractor’s solution shall support canned and ad hoc reporting.

The Contractor shall provide the following Business Intelligence and Reporting:

1. Loan Administration (LA) Reports – The solution provides standard reports for Central Office LA and RLC management for overseeing LA program operations;
2. Additional VA Functional Reports – The solution provides standard reports for other VA entities such as Administrative and Loan Accounting Center (ALAC), the Debt Management Center (DMC), Loan Production (LP), Monitoring Unit (MU), and Property Management (PM);
3. Servicer Operational Reports – The solution provides standard reports to servicers, as referenced in the Reporting Library (See Attachment E, VALERI Reporting Library, for examples of reports); and
4. Business Intelligence (currently known as VALERI Data Mart and servicer tier-ranking reports) – The solution presents VA users with the ability to create and export ad-hoc reports on demand, and with user defined data. All data elements captured by VALERI are available for reporting purposes, in addition to various calculations performed by the solution. The Data Mart shall include four (4) focus areas: Workload Metrics, Portfolio Analytics, Executive Dashboard and Servicer Tier-Ranking.

**Deliverables:**

1. Ad-hoc Reports
2. LA Reports
3. Functional Reports
4. Servicer Operational Reports
5. Business Intelligence Reports

### SERVICER ANALYSIS

VA has developed a tier-ranking program, which evaluates and ranks the performance of VA servicers but has not deployed due to incomplete regulations. The Contractor’s solution shall support VA by implementing a servicer tier-ranking program, including an analytics tool capable of identifying environment-wide, servicer specific and loan level trending to support VA in improving program performance. (See ATTACHMENT G – Tier Ranking Requirements for additional information.) The tools provided and associated maintenance activities shall include:

1. Providing and maintaining a model and tool that supports VA criteria for tier-ranking of servicers and analysis of VA portfolio;
2. Collecting servicer performance data, based on established VA ranking criteria, to include timeframes, appropriate servicing actions, and adherence to VA regulations;
3. Maintaining a tool for comparison of VA portfolio data to data reported from the servicing industry on VA portfolio loans for the purposes of verifying quality of data (VA loan count, balances, statuses, delinquency stages, foreclosures, loss mitigation efforts);
4. Comparing VA portfolio statistics to other Federal home loan programs, [*i.e.,* Fannie Mae (FNMA), Federal Home Loan Mortgage Corporation (FHLMC), *etc*.] portfolio statistics;
5. Maintaining a tier-ranking Scorecard;
6. Maintaining the algorithms and reporting (metrics, weighting, calculations);
7. Supporting infrastructure (data processing, servers, edit checks, data integrity);
8. Proactively resolving issues related to data format, structure, and quality;
9. Incorporating any additional validation and quality measures provided by VA;
10. Providing and aggregating loan level data based on VA requirements;
11. Providing the reporting of aggregate month-end mortgage servicing data and metrics;
12. Working with VA to develop recurring reports as defined by VA to include Scorecard Tier-Ranking reports; and
13. Creating and modifying all report templates as defined by VA.

**Deliverable:**

1. Quarterly Servicer Tier-Ranking Reports

### TESTING

The Contractor shall conduct the necessary testing of the service, and subsequent enhancements, to provide a defect free user experience.

### TEST PLAN

The Contractor shall provide a thorough Test Plan and provide VA the plan for approval 1 day or more prior to testing. Additionally, the Contractor shall provide the facility and equipment to host UAT to validate the solution’s functionality compliance with VA requirements. VA will approve the Test Plan prior to the execution of that plan.

**Deliverable:**

1. Test Plan

### TEST SCENARIOS AND SCRIPTS

The Contractor’s shall develop test scenarios and scripts to support the Test Plan, which shall be submitted to VA for approval. After all testing has been conducted; the Contractor shall provide test results that detail the test conducted and the outcomes of those tests.

**Deliverables:**

1. Test Scenarios and Scripts
2. Test Results

### LIMITED USE PILOT OF PRODUCTION VALERI SOLUTION

Prior to deployment to the production environment, the Contractor shall execute a limited-use pilot to test the solution during the transition phase to ensure that the intended outcome, as specified by VA, was achieved. The pilot shall include representatives of all user types, including SWP users and direct connect. This pilot shall mirror the actual production environment of the solution using live data. The pilot results shall be submitted to VA for approval prior to migration for all mortgage servicers and VA users. Successful completion of the pilot shall require the Contractor to execute, and provide evidence of, successful transactions/interactions of all requirements contained within this PWS. The Contractor shall ensure that new software bugs/defects are minimized, maintaining a ratio of new defects to number of enhancements per release does not exceed 1:30.

### “ALL USER” IMPLEMENTATION

After the pilot is complete and VA has approved deployment for all users, the solution shall be deployed according to the schedule in the PMP. The Contractor shall provide a progressive release schedule based on the solution performance.

The implementation schedule shall be proposed by the Contractor to VA for approval.

### DISASTER RECOVERY (DR)

The Contractor shall provide solution that has full DR capabilities for of all VALERI equipment and software to ensure that the solution is available. The Contractor shall provide a DR Plan and environment that mirrors production for continuous backup of VALERI data to provide uninterrupted user experience should a disaster occur. The Contractor shall be responsible for meeting the organization’s Recovery Point Objective (RPO) of zero (0) loss of data or transactions and Recovery Time Objective (RTO) of 5 minutes. This includes ensuring all software maintenance releases and solution enhancements are applied to the DR and production environment on a timely basis. The Contractor shall provide a monthly report on database activities and back-ups.

**Deliverables:**

1. DR Plan
2. DR Environment
3. Monthly Database and Back-up Reports

### USER TRAINING

The Contractor shall provide a comprehensive, on-going, role-specific training for new and existing VALERI users to provide them with the necessary skills and knowledge to perform their roles in the VALERI environment. The roles shall align with the SRS. At a minimum, the Contractor shall provide the following:

1. A VA-approved training strategy and Training Plan for all Contractor employees including, newly assigned contractor staff as well as sub-contractors, created during the Transition period and for future additions to replace or supplement existing staff;
2. Pre-recorded modular web-based training for all aspects of features and functionality available 24/7 linked to the solution;
3. Train-the-Trainer (T3) materials and curriculum created and delivered during the transition period and when new releases affecting user experience occur (an electronic copy of the materials shall be available for all participants 24 hours prior to the scheduled training session);
4. Regularly updated web-based User Manual describing how to use the solution;
5. Regularly updated web-based Questions and Answers (Q&As);
6. Needs-based on-site tailored training for specific mortgage servicers (VA anticipates no more than six (6) training sessions per year to commence in the first option period), an electronic copy of the materials shall be available for all participants 24 hours prior to the scheduled training session;
7. No more than two (2) T3 sessions for VA personnel, at Contractor facilities prior to deployment (an electronic copy of the materials shall be available for all participants 24 hours prior to the scheduled training session); and
8. Update training material as enhancements and upgrades are made to the solution.

**Deliverables**

1. Training Strategy and Plan
2. Train-the-Trainer (T3) materials
3. Training Material
4. Web-based User Manual
5. Q&As
6. On-site Training and related materials

## OPERATE, MAINTAIN AND ENHANCE VALERI SOLUTION

The Contractor shall provide on-going maintenance and necessary enhancements of all resources required to maintain VALERI in a manner consistent with industry standards. Enhancements may include, but are not limited to, maintenance and upgrades associated with hardware, interfaces, and software. This includes ensuring all software maintenance releases and solution enhancements are applied to the DR and production environment. Any solution (or release) impacting user experience requires prior notice and VA approval. Scheduled changes shall be communicated to VA five (5) business days in advance of the change. Schedule one (1) release every eight (8) weeks as directed by the COR and documented in the PMP. Interim releases shall be required for high priority issues. No more than two (2) releases rescheduled per year.All deployments, including system maintenance and releases, shall be performed during non-business hours between the hours of 10 p.m. ET to 6 a.m. ET on Friday, Saturday or Sunday. Unscheduled changes required to restore user experience do not require advance notice, however shall require after-action notice reporting to VA. The Contractor shall provide on-going pre-recorded refresher training and training for new users. The Contractor shall ensure that it follows industry standards for managing changes to the solution. The Contractor shall provide its Change Management Plan, including relevant performance metrics, at the Quarterly Change Control Board (CCB) meetings, which the Contractor shall host, and provide meeting minutes. Release specific Change Management Plan shall be submitted to VA for approval prior to the scope of every release being defined. All decisions will be vetted through the CCB for approval.

The Contractor shall continuously update and enhance information and functionality made available to VA and the performance of their solution, consistent with any updates made to its COTS product and/or consistent with industry standards. Examples may include the addition of hardware to improve page loads, refining the GUI to improve usability, addition of new functionality, the addition of interfaces into Department of Defense systems to determine Service Members Civil Relief Act (SCRA) eligibility, *etc*. The Contractor shall provide necessary updates in accordance with Federal, state, jurisdictional law, new regulations, *etc*. The Contractor shall conduct on-going testing (refer to Section 5.3.1) to verify these updates and enhancements functions properly and does not have any negative effects on the core program. The Contractor shall also maintain an industry standard for technology utilized by the solution including hardware, software, interfaces, and coding language.

**Deliverables:**

1. After-Action Notice Reports
2. Change Management Plan
3. CCB Meeting Minutes

### ON-GOING TESTING

The Contractor shall provide testing throughout the life of this contract in compliance with Project Management standards (refer to PMBOK in Section 2.0) established in this PWS. The testing shall include functional and technical upgrade testing and imitate the production environment. The UAT testing environment shall be refreshed with each solution release. Additionally, the Contractor shall provide facility and equipment to host UAT to validate solution functionality compliance with VA requirements.

**Deliverable:**

1. Ongoing Testing Results

### CUSTOMER SERVICE/HELP DESK SUPPORT/TICKET TRACKING

The Contractor shall provide second-level customer service support via phone, email and/or chat for designated first-level customer support personnel. First level customer support personnel are comprised of VALERI subject matter experts employed by the VA (known as Regional Loan Center Points of Contact (RLC POCs) or within the Mortgage Servicing companies that are registered users of VALERI. VALERI subject matter experts in VA’s Loan Guaranty Service Central Office (VACO) shall also be supported by the second level customer service support provided by the Contractor.

Prior to transitioning into the Contractor’s solution shall provide advanced defect tracking, and training. The Contractor shall continue providing second-level customer support service throughout the duration of the contract. Customer support services for the Contractor’s solution shall ensure issues that inhibit the use of the VALERI services to perform its loan servicing and payment activities are documented and resolved. If there are any issues identified by VA and communicated to the Contractor, the Contractor shall track each issue and its resolution. The Contractor shall provide a monthly Help Desk Executive Summary Report identifying the number of help desk tickets opened and closed and indicate any trending issues by the third (3rd) business day of every month.

At a minimum, the Contractor shall provide VA with “preferred customer” and priority status on process improvements, information technology, and reporting requests issued against this solicitation.

The Contractor shall perform, at a minimum, the following customer service actions:

1. Provide second-level help desk service support for the mortgage servicing industry and second-level help desk service support, via phone and email at a minimum, for VA personnel and mortgage servicers. Functions shall include, but not be limited to: solution support, defect tracking, enhancement tracking and training. (Note: The Contractor shall not address or respond to any policy issues. Creation of VA personnel credentials and the creation of new servicing companies require approval from authorized VA staff.);
2. Average hold times in any given month shall never exceed industry standards, currently three (3) minutes.  As with any transition, VA anticipates higher call volumes during the transition period, which will decline as user knowledge, available training improves, corrections to solution defects and solution enhancements are implemented.
3. Provide a report on all help desk activities;
4. Understand and recreate issues as reported (shall use VALERI solution to research and resolve issues);
5. Research and track development, communication, interface, and technical VALERI related-issues and open tickets accordingly;
6. High priority/severity issues, such as global outages, inability to pay claims, resolved shall be resolved with five (5) minutes of discovery;
7. Open, track, and close help desk issues through resolution;
8. Reduce the number of outstanding defects by 10% ever quarter and provide evidence of that progress in the MSR.
9. Manage solution enhancement and defect resolution (conduct review of priorities, host weekly calls, verify issue resolution, *etc*.);
10. Create Root Cause Analysis (RCA) for critical VALERI issues including, but not limited to, issues that result in an actual or potential financial loss to the Government; and
11. Host a weekly outstanding issues call.

**Deliverable:**

1. Monthly Help Desk Executive Summary Reports

## EXIT TRANSITION

The Contractor shall, upon the CO's written notice, (l) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The Exit Transition Plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the CO's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

**Deliverable:**

A. Exit Transition Plan

## OPTION PERIODS

For each option period the Contractor shall perform the following tasks identified in this PWS.

### OPTION PERIOD 1:

For option period 1, the Contractor shall perform tasks identified in Sections and subsections of 5.1, 5.2, 5.3, and 5.4.

### OPTION PERIOD 2:

For option period 2, the Contractor shall perform tasks identified in Sections and subsections of 5.1, 5.2, 5.3, and 5.4.

### OPTION PERIOD 3:

For option period 3, the Contractor shall perform tasks identified in Sections and subsections of 5.1, 5.2, 5.3, and 5.4.

### OPTION PERIOD 4:

For option period 4, the Contractor shall perform tasks identified in Sections and subsections of 5.1, 5.2, 5.3, and 5.4.

# GENERAL REQUIREMENTS

## POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

### POSITION/TASK RISK DESIGNATION LEVEL(S)

| **Position Sensitivity** | **Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, “Personnel Security Suitability Program,” Appendix A) |
| --- | --- |
| **Low** | **National Agency Check with Written Inquiries (NACI)** A 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** | **Moderate Background Investigation (MBI)** A 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** | **Background Investigation (BI)** A 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, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree. |

|  |  |
| --- | --- |
|  | **Position Sensitivity and Background Investigation Requirements** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Task Number** | Low/NACI | Moderate/MBI | 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.

Contractor Responsibilities

1. The Contractor shall bear the expense of obtaining background investigations or reciprocals of previous investigations held that meet or exceed the required investigation level. **The cost of background investigations is based on the current Office of Personnel Management (OPM) rate at the time the application is processed at OPM.** Fiscal Year 2014 rates are as follows: Low Risk (NACI) **$279**, Moderate Risk (MBI) **$989**, High Risk (BI) **$4,225** or Reciprocals are **$30**. VA will pay for investigations or reciprocals processed through the VA SIC and conducted by OPM in advance; however, the Contractor shall reimburse the full cost of background investigations/reciprocals to VA within 30 days of Bill of Collections received from VA. VA shall send up to three plus one final delinquent notice to the Contractor. If the Contractor does not adhere to the Bill of Collections, future invoices may be subject to be offset by VA to recoup background investigation/reciprocal costs.

2. Immediately after contract or task order award, the COR will provide the Contractor with the following background investigation document to be completed by the Contractor and returned to the COR to begin the background investigation process for all contract employees working on the contract who will have access to VA facilities, VA systems, or privacy data:

1. **Background Investigation Request Worksheet**
2. **Optional Form 306 – Declaration of Federal Employment**
3. **Fingerprint Request Form**

3. Upon receipt of the above-stated documents from the COR, the VBA Acquisition Staff will submit the background investigation package to the VSC Security Specialist for processing through the SIC. **Upon notification of favorable fingerprint results, the contractor may begin work while the background investigation is ongoing.** Thereafter, the Contractor will receive an email notification from the VSC or SIC identifying the website link that includes detailed instructions regarding completion of the background clearance application process in the Electronic Questionnaires for Investigations Processing (e-QIP) system. E-QIP is an online, Internet accessible system where the contractor employee shall complete the security questionnaire required for OPM to process the background investigation.

4. Contractors who have a current favorable background investigation previously conducted by OPM or Defense Security Service (DSS) may be accepted through reciprocation. When a previous clearance is currently held, it does not preclude the vendor from submittinga complete Background Investigation Package as stated above to the COR immediately after contract or task order award for all contract employees who will be working on the contract.

5. The Contractor shall prescreen all personnel who require access to VA site(s) and/or access to VA LAN systems to ensure they maintain a U.S. citizenship or Alien Registration that authorizes them to work in the U.S. and are able to read, write, speak and understand the English language.

6. Contract performance **shall not** commence before:

* The VSC has confirmed favorable fingerprint results, **or**
* SIC confirms that it has received the Contractor’s investigative documents, the documents are complete, and that the investigation information has been released to OPM for scheduling of the background investigation, **or**
* VSC or the SIC has confirmed that the verified investigation will be reciprocated.

7. The COR will notify and forward the Contractor a copy of the Certificate of Investigation when the background investigation has been favorably completed or a Certificate of Eligibility (Form 4236) if the investigation has been reciprocated. The Contractor, if notified of an unfavorable adjudication by the Government, shall withdraw the employee from consideration from working under the contract. Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

8. The Contractor will be responsible for the actions of those contract and subcontract employees they provide to perform work for VA. In the event damage arises from work performed by Contractor personnel, under the auspices of the contract, the Contractor will be responsible for resources necessary to remedy the incident.

9. Should the Contractor use a vendor other than OPM or DSS to conduct investigations, the investigative company must be certified by OPM/DSS to conduct Contractor investigations. The Vendor Cage Code number must be provided to the VA SIC, which will verify the information and conclude whether access to the Government’s site(s) and/or VA LAN systems can be granted.

10. The investigative history for Contractor personnel working under this contract must be maintained in the databases of either OPM or the Defense Industrial Security Clearance Organization (DISCO).

### 

## METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

## 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** |
| --- | --- | --- |
| 1. Technical Needs | System is fully functional and available 24/7/365 | System up-time exceeds 99.9% (Section 5.2) |
| High priority/severity issues, such as global outages, inability to pay claims, resolved immediately | Global issues are resolved within five (5) minutes of initial report (Section 5.3.2) |
| System maintenance and releases performed during non-business hours | Releases conducted between the hours of 10 p.m. ET to 6 a.m. ET on Friday, Saturday or Sunday (Section 5.2.6) |
| Count of outstanding defects, consistently decline | 10% decline of outstanding defects, quarter over quarter (Section 5.3.2.8) |
| System releases do not introduce new defects | Ratio of new defects to number of enhancements per release does not exceed 1:30 (Section 5.2.5) |
| Solution is responsive | Page loads average less than .5 second (Section 5.2) |
| 1. Project Milestones and Schedule | Regularly scheduled system release schedule | One (1) release every eight (8) weeks as directed by the COR. Interim releases for high priority issues. No more than two (2) releases rescheduled per year. (Section 5.2.6) |
| Notification of releases | 100% 10-day notification of all scheduled releases (Section 5.2.6) |
| 3. Project Staffing | Seamless transition of resources | Any new staff fully trained and briefed on program and solution prior to assuming role on VALERI team (Section 5.2.8) |
| 4. Value Added | Training issues | Proactively identify and resolve outstanding training issues |
| Suggest enhancements | Using various techniques/resources (helpdesk issues, user forums, user surveys, *etc.*) proactively suggest design enhancements to improve user experience |

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.

## FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis. The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will 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. 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 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. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

## GOVERNMENT FURNISHED PROPERTY

The government will provide electronic records and data necessary to establish the historical actions taken by or documented by the VA, in relation to specific loans contained within the existing VALERI environment. The contractor will be responsible for merging this information with any newly acquired information, on a loan level basis, or otherwise, as it relates to the requirements herein. This imported data shall be available in the production version of the Contractor’s solution at all times.

## RIGHTS IN DATA

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government Agency or Government Contractor, which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others.

Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the CO. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner, which provides for greater rights to the Contractor.

VA shall have unlimited rights to and ownership of all deliverables provided under this effort, including reports, recommendations, briefings, work plans, and all other deliverables. This includes the deliverables provided under the basic award, as well as any optional task deliverables that are exercised by the CO. The definition of “unlimited rights” is contained in FAR 27.401, Definitions.

## ACRONYM LIST

| **ACRONYM** | **DEFINITION** |
| --- | --- |
| ADA | Americans with Disabilities Act |
| ALAC | Administrative and Loan Accounting Center |
| BCP | Business Continuity Plan |
| BI | Background Investigation – High Risk |
| BOC | Bills of Collection |
| CCB | Change Control Board |
| CD-ROM | Compact Disc, read-only-memory |
| CFR | Code of Federal Regulations |
| CLIN | Contract Line Item Number |
| CO | Contracting Officer |
| COR | Contracting Officer’s Representative |
| COTS | Commercial-off-the-Shelf |
| CPTS | Centralized Property Tracking System |
| D.C. | District of Columbia |
| DIL | Deed-in-Lieu |
| DISCO | Defense Industrial Security Clearance Organization |
| DMC | Debt Management Center |
| DR | Disaster Recovery |
| DSS | Defense Security Service |
| e-QIP | Electronic Questionnaires for Investigations Processing System |
| FAR | Federal Acquisition Regulation |
| FFP | Firm Fixed Price |
| FHLMC | Federal Home Loan Mortgage Corporation |
| FISMA | Federal Information Security Management Act |
| FMS | Financial Management System |
| FNMA | Fannie Mae |
| FTR | Federal Travel Regulations |
| FY | Fiscal Year |
| GSA | General Services Administration |
| GUI | Graphical User Interface |
| HUB | Historically Underutilized Business |
| IE | Internet Explorer |
| ISO | Information Security Officer |
| IT | Information Technology |
| JPEG | Joint Photographic Expert Group |
| LA | Loan Administration |
| LAN | Local Area Network |
| LGY | Loan Guaranty Service |
| LP | Loan Production |
| LPS | Lender Processing Services |
| MBI | Moderate Background Investigation – Moderate Risk |
| MS | Microsoft |
| MSR | Monthly Status Report |
| MU | Monitoring Unit |
| NACI | National Agency Check with written Inquires – Low Risk |
| NARA | National Archives and Records Administration |
| NIST | National Institute of Standards and Technology |
| NLT | No Later Than |
| NSF | National Standard Format |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| PDF | Portable Data Format |
| PII | Personally Identifiable Information |
| PM | Property Management |
| PMP | Project Management Plan |
| POC | Point of Contact |
| PS | Project Schedule |
| PWS | Performance Work Statement |
| Q&A | Questions and Answers |
| QA | Quality Assurance |
| QAP | Quality Assurance Plan |
| QC | Quality Control |
| QCP | Quality Control Plan |
| RCA | Root Cause Analysis |
| RLC | Regional Loan Center |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SB | Small Business |
| SDVOSB | Service Disabled Veteran Owned Small Business |
| SIC | Security and Investigations Center |
| SOPs | Standard Operating Procedures |
| SPI | Sensitive Personal Information |
| SRS | Software Requirements Specifications |
| SWP | Servicer Web Portal |
| T3 | Train-the-Trainer |
| T&I | Taxes and Insurance |
| T&M | Time and Materials |
| TAS | The Appraisal System |
| TFM | Treasury Financial Manual |
| TMS | Talent Management System |
| TO | Task Order |
| TOA | Task Order Award |
| TROR | Treasury Report on Receivables |
| U.S. | United States |
| U.S.C. | United States Code |
| VA | Veterans Affairs |
| VAAR | Veterans Affairs Acquisition Regulation |
| VACO | Veterans Affairs Central Office |
| VALERI | Veterans Affairs Loan Electronic Reporting Interface |
| VANTS | VA Nationwide Teleconferencing System |
| VBA | Veterans Benefits Administration |
| VHA | Veterans Health Administration |
| VOSB | Veteran Owned Small Business |
| webLGY | Web-enabled Loan Guaranty System |
| WOSB | Woman-Owned Small Business |

## LIST OF ATTACHMENTS

ATTACHMENT A – Servicing System Interface Document

ATTACHMENT B – VALERI Technician Guide

ATTACHMENT C – LGY Business Rules

ATTACHMENT D – VALERI Reporting Library

ATTACHMENT E – Software Requirements Specifications (SRS)

ATTACHMENT F - Process And Steps For All Active Processes

ATTACHMENT G – Tier Ranking Requirements

ATTACHMENT H – Security Deliverables

# ADDENDUM A

1. 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 Project Manager, 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](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.

1. VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP).  VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

* 1. **VA Internet and Intranet Standards:**

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

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

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

1. 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 are 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.

**Section 508 – Electronic and Information Technology (EIT) Standards:**

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <http://www.section508.gov> and <http://www.access-board.gov/sec508/standards.htm>. A printed copy of the standards will be supplied upon request.  The Contractor shall comply with the technical standards as marked:

\_x\_§ 1194.21 Software applications and operating systems

\_x\_§ 1194.22 Web-based intranet and internet information and applications

\_x\_§ 1194.23 Telecommunications products

\_x\_§ 1194.24 Video and multimedia products

\_x\_§ 1194.25 Self contained, closed products

\_x\_§ 1194.26 Desktop and portable computers

\_x\_§ 1194.31 Functional Performance Criteria

\_x\_§ 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

1. Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed.  It is the responsibility of the Contractor to park in the appropriate designated parking areas.  VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.
6. 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 toProtected 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 Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information.  Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities.  Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract.  Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature.  If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract*,* the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information.  Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives.  The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. 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.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. 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.
17. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed.  In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

# ADDENDUM B

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

1. 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.

1. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
   1. 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.
   2. 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.
   3. 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.
   4. 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, 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.
   5. The Contractor or Subcontractor must notify the Contracting Officer 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 Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.
2. VA INFORMATION CUSTODIAL LANGUAGE
3. 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).
4. 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.
5. 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 Contracting Officer within 30 days of termination of the contract.
6. 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.
7. 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 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.
8. 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.
9. 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 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
10. 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.
11. 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.
12. 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 contracting officer for response.
13. 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 contracting officer for response.
14. 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.
15. INFORMATION SYSTEM DESIGN AND DEVELOPMENT
16. 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*). 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*.
17. 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.
18. 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.
19. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
20. 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*.
21. 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.
22. The Contractor/Subcontractor agrees to:
    1. 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:
       1. The Systems of Records (SOR); and
       2. The design, development, or operation work that the Contractor/Subcontractor is to perform;
    2. 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
    3. 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
23. 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.
    1. “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.
    2. “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.
    3. “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.
24. 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.
25. 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 availability of the system). Such issues shall be remediated as quickly as is practical**,** based upon the severity of the incident.
26. 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 severity of the incident.
27. 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 contracting officer and the VA Assistant Secretary for Office of Information and Technology.
28. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE
    1. 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 reviewed and approved by VA prior to implementation.
    2. 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.
    3. 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.
    4. 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 contracting officer 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.
    5. 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.
    6. 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.
    7. 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.
    8. 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:
29. Vendor must accept the system without the drive;
30. 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
31. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
32. 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;
33. 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
34. 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.
35. 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.
36. SECURITY INCIDENT INVESTIGATION
    1. 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.
    2. 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.
    3. 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.
    4. 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.
37. LIQUIDATED DAMAGES FOR DATA BREACH
    1. 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.
    2. 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.
    3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
       1. Nature of the event (loss, theft, unauthorized access);
       2. Description of the event, including:
       3. date of occurrence;
       4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
       5. Number of individuals affected or potentially affected;
       6. Names of individuals or groups affected or potentially affected;
       7. 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;
       8. Amount of time the data has been out of VA control;
       9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
       10. Known misuses of data containing sensitive personal information, if any;
       11. Assessment of the potential harm to the affected individuals;
       12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
       13. 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.
    4. 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:
       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.
38. SECURITY CONTROLS COMPLIANCE TESTING

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

1. TRAINING
2. 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. Sign and acknowledge (either manually or electronically) 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 the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
     3. Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;
     4. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
     5. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
3. The Contractor shall provide to the contracting officer 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. These online courses are located at www.tms.va.gov. To self-enroll, click the “Create New User” button on the red bar and complete the assigned training. The COR will provide the contractor with the appropriate information to complete self-enrollment. Technical issues with TMS should be directed to the TMS help desk at vatmshelp@va.gov or 1.866.496.0463.
4. Failure to complete the mandatory annual training and 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.