

Beneficiary Travel Self-Service System (BTSSS)

Requirements Specification Document



November 2015

Version 2.0

Department of Veterans Affairs

Revision History

Note: The revision history cycle begins once changes or enhancements are requested after the Requirements Specification Document has been baselined.

Date	Version	Description	Author
11/06/2015	2.0	Final Draft	Engility
11/04/2015	1.6	Updated Section 2.13	Engility
10/21/2015	1.5	Removed Epic tables; incorporated Epic tables into the BTSSS RTM	Engility
10/15/2015	1.4	Draft review with VA IPT team	Engility
10/14/2015	1.3	Final draft of Epic tables for functional requirements.	Engility
10/5/2015	1.2	Reworking Non-Functional Requirements	Engility
9/29/2015	1.1	Reworking Functional Business Requirements	Engility
09/25/2015	1.0	Initial Draft	Engility

Artifact Rationale

The Requirements Specification Document (RSD) records the results of the specification gathering processes carried out during the Requirements phase. The RSD is generally written by the functional analyst(s) and should provide the bulk of the information used to create the test plan and test scripts. It should be updated for each increment.

The level of detail contained in this RSD should be consistent with the size and scope of the project. It is not necessary to fill out any sections of this document that do not apply to the project. The resources necessary to create and maintain this document during the life cycle of a large project should be acknowledged and clearly reflected in project schedules. Do not duplicate data that is already defined in another document or in a section in this document; note in the section where the information can be found.

Instructions

Activity	New Capability (1)	Feature Enhancement (2)
Field Deployment (A)	Yes	Yes
Cloud/Web Deployment (B)	Yes	Yes
Mobile Application (C)	Yes	Yes

Table of Contents

1. Introduction	1
1.1. Purpose	1
1.2. Scope.....	1
1.3. References	1
2. Overall Description.....	2
2.1. Accessibility Specifications	2
2.2. Business Rules Specification	3
2.3. Design Constraints Specification	3
2.4. Disaster Recovery Specification	3
2.5. Documentation Specifications.....	4
2.6. Functional Specifications	5
2.7. Graphical User Interface (GUI) Specifications	5
2.8. Multi-divisional Specifications	5
2.9. Performance Specifications	5
2.10. Quality Attributes Specification	5
2.11. Reliability Specifications	6
2.12. Scope Integration.....	6
2.13. Security Specifications.....	6
2.14. System Features.....	15
2.15. Usability Specifications	15
3. Purchased Components	15
4. Estimation	16
5. Approval Signatures	18
Appendix A: Non-Functional Requirements	19

1. Introduction

The Department of Veterans Affairs (VA) operates the nation's largest integrated health care network, operating over 150 hospitals, over 130 community living centers and over 900 outpatient clinics. There are over 8.5 million Veterans enrolled in the VA health care system, with over 5.5 million Veterans using the health care system in any given year.

As part of its commitment to ensuring that Veterans have adequate access to VA health care facilities, the VA provides mileage reimbursement to eligible Veterans to offset costs associated with travel to hospitals.

In Fiscal Year (FY) 2010, the VA provided mileage reimbursement to one million eligible beneficiaries. As part of its commitment to Veterans and to the American public to serve as good stewards of public resources, the VA seeks to make improvements to the Beneficiary Travel (BT) program under the Beneficiary Travel Self-Service System (BTSSS) solution.

1.1. Purpose

The Requirements Specification Document (RSD) specifies the functions, business rules, data, and technology that are to be implemented by the BTSSS. The purpose of this document is to capture and articulate the Functional and Non-Functional Requirements of the BTSSS solution. The intended audience is both the business community, who supplies and approves the requirements, and the developer who will provide the software and hardware that will make up the BTSSS solution. This document serves as the baseline to further define the scope of the project and verify the quality of the solution.

1.2. Scope

The scope of this document is to cover the software requirements for the BTSSS that are to be deployed to a VA-approved data center. The BTSSS consists of a commercial-off-the-shelf (COTS) program for processing mileage, transportation, meals, and lodging expenses. This solution is to be interfaced with existing VA systems that provide Veteran information, identity and access control, and electronic funds transfer (EFT) information. The system needs to be capable of handling mileage reimbursements, as well as meals, lodging, and other approved special transportation methods. For items other than mileage reimbursement, receipts will be required. The BTSSS also needs to be able to handle the processing of scanned receipts. The BTSSS solution needs to be web-based and capable of being integrated with self-service portals such as MyHealtheVet and eBenefits, as well as VA Kiosks located in VA medical facilities.

1.3. References

The following reference documents served as inputs to this RSD;

- [BTSSS Business Requirements Document \(BRD\) NSR ID #20120202](#)
- [US Code Title 38 Section 111 \(38 U.S.C 111\) - Payments or allowances for Beneficiary Travel](#)
- [Code of Federal Regulations Title 38 Part 70](#)
- [VHA Handbook 1601B.05, "Beneficiary Travel"](#)

- [Beneficiary Travel Fact Sheet](#)
- [Beneficiary Travel Brochure](#)
- [Beneficiary Travel Frequently Asked Questions](#)
- [VA Handbook 6500 – Information Security Program](#)
- [VistA Beneficiary Travel Manuals \(Installation, Technical, User\)](#)

2. Overall Description

The BTSSS will provide features and capabilities that leverage automation and multiple-user interface capabilities to manage and process Beneficiary Travel claims.

The BTSSS will need to provide many of the features and capabilities found in the typical third-party expense management services and solutions.

These can be summarized as:

- The ability to create a user profile with contact and financial information; used for EFT payment.
- The ability to create expense entries.
- The ability to upload scanned images of receipts and supporting documentation and link these to the expense entries.
- The ability to plan for future Beneficiary Travel.
- The ability to submit expenses for either manual or automatic review for approval.
- The ability to receive the payment in the form of an EFT transaction.
- The ability to improve Business Intelligence and Reporting.

The main difference between the BTSSS and the typical third-party expense management services and solutions, is the need to evaluate claims based on the VA Beneficiary Travel rules and guidelines and using Medical Appointment and Eligibility information found in external systems.

2.1. Accessibility Specifications

Accessibility specifications are functional and technical standards that are built-in to the BT system and are required by Federal law. Section 508 of the Rehabilitation Act (29 U.S.C. 794d) as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, mandates that all electronic and information technology developed, procured, maintained, or used by the Federal Government be accessible to people with disabilities. Technology is considered to be “accessible” if it can be used as effectively by persons with disabilities, as well as those persons who are not disabled.

Section 508 of the Americans with Disabilities Rehabilitation Act Amendment requires that Federal departments and agencies ensure that electronic and information technology (IT) is accessible to people with disabilities, unless an undue burden would be imposed on the department or agency.

This Section focuses primarily on Federal pages on the Internet and the Intranet, but also includes guidance for disseminating information, using computer hardware and software.

The VA's engineers within the Department of Product Development Product Assessment Competency Division, test proposed E&IT (Electronic and Information Technology) products for Section 508 conformance within the VA's Enterprise Architect Framework. The VA's compliance with Section 508 means ensuring interactions with Veterans and internal operations in the VA, are within the standard.

As a subdivision of VA, the Veteran Health Administration's (VHA's) accessibility specifications must comply with the VA's standards. Systems that are designed from the onset of an idea, or modified from an existing system, must comply. The VHA Web pages must comply with the VA Directive and Handbook 6102, Internet/Intranet Services. The directive requires the VA to maintain a central database that identifies all Web sites and the person(s) responsible for the content and technical aspects.

2.2. Business Rules Specification

The business rules applicable to BTSSS are codified in the Code of Federal Regulations (CFR) and expanded upon within the Beneficiary Travel Guidelines. A detailed breakdown of some of the eligibility and calculation business rules, along with their associated CFR and/or Beneficiary Travel guidelines, can be found in the BTSSS BRD document under the "Appendix A – References" section.

2.3. Design Constraints Specification

The following items represent mandated design decisions that have been made regarding the design and development of the BTSSS. The majority of these requirements revolve around the existing VA enterprise licenses for software, and the VA's desire to reduce licensing costs by utilizing these licenses for new initiatives, where possible.

With regard to supported web browsers, the expectation is that the BTSSS will be a web-based system with a large user base across the many VA facilities. Therefore, we require that the software be able to run within the approved browsers used in the VA, without the need for custom plugins that would be difficult to manage on hundreds of thousands of computers.

Agile development methodologies, including a scrum management framework, will be utilized for development using a cross-functional team. Fixed-length iterations will be employed with applicable testing. Each iteration will provide an opportunity for early business-owner feedback to ensure compliance with the required specifications.

2.4. Disaster Recovery Specification

The BTSSS will comply with, and operate under, the VA Authority to Operate (ATO) issued to the Repositories Project. The BTSSS operates on hardware that is owned and managed by the Repositories Project; therefore any and all Disaster Recovery (DR) protocols and intervention are owned and managed by the Repositories Project.

The Production systems are currently hosted out of (to be provided in the future) by Veterans Transportation Program (VTP). Failover systems shall be hosted out of (to be provided in the

future) by VTP. The BTSSS falls under the reliability and performance specifications in place for the Repositories Project.

All documentation related to data repositories, protocols, and interventions are owned by the Repositories Project and can be located on the VA Software Document Library (VDL).

- The BTSSS shall comply with all applicable Federal, VA, and VHA rules and regulations for the archival and storage requirements of the data processed, which is a minimum of seven years.
- A back-up plan will be provided for when the system is brought off-line for maintenance or technical issues/problems.
- Data protection measures, such as back-up intervals and redundancy, shall be consistent with systems categorized as Semi-critical.
Note: Data protection measures should include encrypting bank information collected by the BTSSS registration process using Advance Encryption Standard as required by Federal Information Processing Standards (FIPS) 197, and that the encryption module implementing Advanced Encryption Standard (AES) must be certified in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules. See VA Handbook 6500 Appendix D SC-8, SC-13, and SC-14.
- Upon execution of disaster recovery procedures, the BTSSS shall be brought back into operation within a 48-hour Disaster Recovery Period.

2.5. Documentation Specifications

The BTSSS development team will adhere to documentation requirements as required by the Project Management Accountability System (PMAS) to comply with the VA and Product Development (PD) documentation standards and/or ProPath requirements. The ProPath templates will be used to document requirements, use cases, interface controls, design specifications, security plans, and project management and implementation specifications. Rational RequisitePro will be used to track requirements and use cases. All project documentation will be stored in Rational ClearCase. This will potentially include, but is not limited to:

- **BTSSS Claimant Users Guide** – descriptions and instructions of Claimant accessible functionality.
- **BTSSS Travel Clerk Users Guide** – descriptions and instructions of Travel Clerk accessible functionality.
- **BTSSS System Administrators Guide** – descriptions and instructions of System Administrator accessible functionality.
- **BTSSS Interface Control Documents (ICDs)** – ICDs specifying how BTSSS communicates with VA and third-party systems.
- **BTSSS Application Programming Interfaces (APIs)**– Documentation of APIs available for third-party developers to access BTSSS.
- **BTSSS Frequently Asked Questions (FAQs) Document** - A document that supplies an end user with standard questions and answers that are frequently asked for a specific task or project.
- **Help Screens** – available for an individual to seek instructions /assistance while accessing the BTSSS system.

2.6. Functional Specifications

The functional business requirements correspond to the epic stories that are included in the Business Requirements Document (BRD). The epic stories are the business needs for the BTSSS project. The user stories are the detailed functional specifications and they are mapped to the epic stories. For details of the functional specifications for the BTSSS project, please refer to the [BTSSS Requirements Traceability Matrix \(RTM\)](#).

2.7. Graphical User Interface (GUI) Specifications

The BTSSS depends on the availability of the host site and associated hardware to support BTSSS as an enterprise-wide Graphic User Interface (GUI).

2.8. Multi-divisional Specifications

A centrally deployed BTSSS instance will offer the functionality to be used in a multi-divisional, integrated site environment.

2.9. Performance Specifications

Performance is concerned with characteristics such as throughput, response time, recovery time, start-up time, and shutdown time. Performance-related activities, such as testing and tuning, are concerned with achieving response times, throughput, and resource-utilization levels that meet the performance objectives for the application under test.

Following are some of the performance requirement specifications that the BTSSS shall meet in order to achieve expectation standards at the VA.

2.10. Quality Attributes Specification

Processes for artifact delivery will follow ProPath guidelines, including quality gate reviews for requirements, design, code, test plans/cases/executions, and other document deliverables.

The BTSSS complies with the quality specifications set forth by the VA PMAS Quality specifications.

The following types of testing will be performed to assess the quality of the solution:

- Unit testing
- Integration / functional testing
- User Acceptance Testing (UAT)
- Section 508 testing
- Performance testing

The BTSSS also consists of the following quality specifications:

- The system is composed of tools, applications, and software that conform to the VA's standard server and database operating systems. The VA [Technical Reference Model \(TRM\)](#) provides more information.
- The system is designed to operate in VA's standard virtualized operating system environment according to the VA [TRM](#).

2.11. Reliability Specifications

The BTSSS solution will need to meet availability requirements as defined by the VA for this type of field-deployed system.

The following summarizes the requirements for BTSSS reliability specifications.

- Availability – the BTSSS shall be available 24/7.
- Mean Time To Repair (MTTR) – System down time shall be a maximum of 24 hours depending on the nature of the failure. For example, if the servers that are allocated to the BTSSS go down (for whatever reason) it is likely they could be brought back on line in a 24-hour period because the problem would be relegated to the servers themselves and not to some kind of environmental catastrophe. If the failure is due to a more widespread problem, such as a fabric failure at Corporate Data Center Operations (CDCO)- Martinsburg, the down time could be greater than 24 hours.
- Accuracy – The BTSSS shall return entries exactly as they were passed with no modification.
- Defect repair – It is expected that all defects related to the implementation will get resolved during initial development and subsequent UAT testing.
- When the system goes live in Production, the BTSSS development team will address defects of a critical nature that are deemed “show stoppers.” Enhancement requests made after go-live will be logged for consideration in a future, coordinated, BTSSS release.

2.12. Scope Integration

As of January 2012, there have been enhancements to the existing Beneficiary Travel package that resulted in changes to the Veterans Health Information Systems and Technology Architecture (VistA), Enrollment System Redesign (ESR), EFT, the Financial Management System (FMS), and other dependent systems. Therefore, the BTSSS project stakeholders will need to continue to review and coordinate these efforts during design, development, implementation, and rollout.

2.13. Security Specifications

The Federal Information Processing Standard 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, defines the security categories, security objectives, and impact levels to which National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 Revision 1, maps information types. A FIPS 199 analysis was completed for the proposed Beneficiary Travel Self-Service System (BTSSS), and it has been determined that the security categorization is **HIGH** in accordance with FIPS 199.

The Security Categorization will drive the initial set of minimal security controls required for the information system. Minimum security control requirements are addressed in NIST SP 800-53 and VA Handbook 6500, Appendix F. All VA security requirements as defined in VA Handbook 6500 Appendix F will be adhered to.

All Enterprise Identity Management requirements will be adhered to. The BTSSS system shall leverage the Enterprise Identity Access Services to manage and enforce VA and Veteran security. The BTSSS system will provide the ability for users to gain access to BTSSS with valid PIV credentials, or a username and password.

The tables below (for management controls, operational controls, technical controls, and privacy controls, respectively) include the relevant references, publications, and directives based on each categorization.

Table 2-1: Security Specifications –High Impact Controls

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	AC-1	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
AC-2	ACCOUNT MANAGEMENT	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)	
AC-3	ACCESS ENFORCEMENT	AC-3	
AC-4	INFORMATION FLOW ENFORCEMENT	AC-4	
AC-5	SEPARATION OF DUTIES	AC-5	
AC-6	LEAST PRIVILEGE	AC-6 (1) (2) (3) (5) (9) (10)	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	
AC-8	SYSTEM USE NOTIFICATION	AC-8	
AC-10	CONCURRENT SESSION CONTROL	AC-10	
AC-11	SESSION LOCK	AC-11 (1)	
AC-12	SESSION TERMINATION	AC-12	
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	
AC-17	REMOTE ACCESS	AC-17 (1) (2) (3) (4)	
AC-18	WIRELESS ACCESS	AC-18 (1) (4) (5)	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19 (5)	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	AC-20 (1) (2)	
AC-21	INFORMATION SHARING	AC-21	
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	AT-1	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
AT-2	SECURITY AWARENESS TRAINING	AT-2 (2)	
AT-3	ROLE-BASED SECURITY TRAINING	AT-3	
AT-4	SECURITY TRAINING RECORDS	AT-4	
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-1	
AU-2	AUDIT EVENTS	AU-2 (3)	
AU-3	CONTENT OF AUDIT RECORDS	AU-3 (1) (2)	
AU-4	AUDIT STORAGE CAPACITY	AU-4	
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	AU-5 (1) (2)	
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-6 (1) (3) (5) (6)	
AU-7	AUDIT REDUCTION AND REPORT GENERATION	AU-7 (1)	
AU-8	TIME STAMPS	AU-8 (1)	
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9 (2) (3)(4)	
AU-10	NON-REPUDIATION	AU-10	
AU-11	AUDIT RECORD RETENTION	AU-11	
AU-12	AUDIT GENERATION	AU-12 (1) (3)	
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	CA-1	
CA-2	SECURITY ASSESSMENTS	CA-2 (1) (2)	
CA-3	SYSTEM INTERCONNECTIONS	CA-3 (5)	
CA-5	PLAN OF ACTION AND MILESTONES	CA-5	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
CA-6	SECURITY AUTHORIZATION	CA-6	
CA-7	CONTINUOUS MONITORING	CA-7 (1)	
CA-8	PENETRATION TESTING	CA-8	
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9	
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-1	
CM-2	BASELINE CONFIGURATION	CM-2 (1) (2) (3) (7)	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
CM-3	CONFIGURATION CHANGE CONTROL	CM-3 (1) (2)	
CM-4	SECURITY IMPACT ANALYSIS	CM-4 (1)	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5 (1) (2) (3)	
CM-6	CONFIGURATION SETTINGS	CM-6 (1) (2)	
CM-7	LEAST FUNCTIONALITY	CM-7 (1) (2) (5)	
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	CM-8 (1) (2)(3)(4) (5)	
CM-9	CONFIGURATION MANAGEMENT PLAN	CM-9	
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10	
CM-11	USER-INSTALLED SOFTWARE	CM-11	
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	CP-1	
CP-2	CONTINGENCY PLAN	CP-2 (1) (2) (3) (4)(5) (8)	
CP-3	CONTINGENCY TRAINING	CP-3 (1)	
CP-4	CONTINGENCY PLAN TESTING	CP-4 (1) (2)	
CP-6	ALTERNATE STORAGE SITE	CP-6 (1) (2) (3)	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
CP-7	ALTERNATE PROCESSING SITE	CP-7 (1) (2) (3) (4)	
CP-8	TELECOMMUNICATIONS SERVICES	CP-8 (1) (2) (3) (4)	
CP-9	INFORMATION SYSTEM BACKUP	CP-9 (1) (2) (3) (5)	
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	CP-10 (2) (4)	
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	IA-1	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	IA-3	
IA-4	IDENTIFIER MANAGEMENT	IA-4	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1) (2) (3) (11)	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
IA-6	AUTHENTICATOR FEEDBACK	IA-6	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8 (1) (2) (3) (4)	
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	IR-1	
IR-2	INCIDENT RESPONSE TRAINING	IR-2 (1) (2)	
IR-3	INCIDENT RESPONSE TESTING	IR-3 (2)	
IR-4	INCIDENT HANDLING	IR-4 (1) (4)	
IR-5	INCIDENT MONITORING	IR-5 (1)	
IR-6	INCIDENT REPORTING	IR-6 (1)	
IR-7	INCIDENT RESPONSE ASSISTANCE	IR-7 (1)	
IR-8	INCIDENT RESPONSE PLAN	IR-8	
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	MA-1	
MA-2	CONTROLLED MAINTENANCE	MA-2 (2)	
MA-3	MAINTENANCE TOOLS	MA-3 (1) (2) (3)	
MA-4	NONLOCAL MAINTENANCE	MA-4 (2)	
MA-5	MAINTENANCE PERSONNEL	MA-5 (1)	
MA-6	TIMELY MAINTENANCE	MA-6	
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	MP-1	
MP-2	MEDIA ACCESS	MP-2	
MP-3	MEDIA MARKING	MP-3	
MP-4	MEDIA STORAGE	MP-4	
MP-5	MEDIA TRANSPORT	MP-5 (4)	
MP-6	MEDIA SANITIZATION	MP-6 (1) (2) (3)	
MP-7	MEDIA USE	MP-7 (1)	
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	PE-1	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
PE-3	PHYSICAL ACCESS CONTROL	PE-3 (1)	
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE-4	
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	PE-5	
PE-6	MONITORING PHYSICAL ACCESS	PE-6 (1) (4)	
PE-8	VISITOR ACCESS RECORDS	PE-8 (1)	
PE-9	POWER EQUIPMENT AND CABLING	PE-9	
PE-10	EMERGENCY SHUTOFF	PE-10	
PE-11	EMERGENCY POWER	PE-11 (1)	
PE-12	EMERGENCY LIGHTING	PE-12	
PE-13	FIRE PROTECTION	PE-13 (1)(2) (3)	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	PE-14	
PE-15	WATER DAMAGE PROTECTION	PE-15 (1)	
PE-16	DELIVERY AND REMOVAL	PE-16	
PE-17	ALTERNATE WORK SITE	PE-17	
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	PE-18	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	PL-1	
PL-2	SYSTEM SECURITY PLAN	PL-2 (3)	
PL-4	RULES OF BEHAVIOR	PL-4 (1)	
PL-8	INFORMATION SECURITY ARCHITECTURE	PL-8	
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	PS-1	
PS-2	POSITION RISK DESIGNATION	PS-2 (3)	
PS-3	PERSONNEL SCREENING	PS-3	
PS-4	PERSONNEL TERMINATION	PS-4 (2)	
PS-5	PERSONNEL TRANSFER	PS-5	
PS-6	ACCESS AGREEMENTS	PS-6	
PS-7	THIRD-PARTY PERSONNEL SECURITY	PS-7	
PS-8	PERSONNEL SANCTIONS	PS-8	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	RA-1	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
RA-2	SECURITY CATEGORIZATION	RA-2	
RA-3	RISK ASSESSMENT	RA-3	
RA-5	VULNERABILITY SCANNING	RA-5 (1) (2) (4) (5)	
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	SA-1	
SA-2	ALLOCATION OF RESOURCES	SA-2	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	
SA-4	ACQUISITION PROCESS	SA-4 (1) (2) (9) (10)	
SA-5	INFORMATION SYSTEM DOCUMENTATION	SA-5	
SA-8	SECURITY ENGINEERING PRINCIPLES	SA-8	
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	SA-9 (2)	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SA-10	
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	SA-11	
SA-12	SUPPLY CHAIN PROTECTION	SA-12	
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	SA-15	
SA-16	DEVELOPER-PROVIDED TRAINING	SA-16	
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	SA-17	
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	SC-1	
SC-2	APPLICATION PARTITIONING	SC-2	
SC-3	SECURITY FUNTCION ISOLATION	SC-3	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
SC-4	INFORMATION IN SHARED RESOURCES	SC-4	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
SC-5	DENIAL OF SERVICE PROTECTION	SC-5	
SC-7	BOUNDARY PROTECTION	SC-7 (3) (4) (5) (7) (8) (18) (21)	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8 (1)	
SC-10	NETWORK DISCONNECT	SC-10	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12 (1)	
SC-13	CRYPTOGRAPHIC PROTECTION	SC-13	
SC-15	COLLABORATIVE COMPUTING DEVICES	SC-15	
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17	
SC-18	MOBILE CODE	SC-18	
SC-19	VOICE OVER INTERNET PROTOCOL	SC-19	
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20	
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	SC-22	
SC-23	SESSION AUTHENTICITY	SC-23	
SC-24	FAIL IN KNOWN STATE	SC-24	
SC-28	PROTECTION OF INFORMATION AT REST	SC-28	
SC-39	PROCESS ISOLATION	SC-39	
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	SI-1	

Control Number	CONTROL NAME	Moderate Impact	VA Guidance
SI-2	FLAW REMEDIATION	SI-2 (1) (2)	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
SI-3	MALICIOUS CODE PROTECTION	SI-3 (1) (2)	
SI-4	INFORMATION SYSTEM MONITORING	SI-4 (2) (4) (5)	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5 (1)	
SI-6	SECURITY FUNCTION VERIFICATION	SI-6	
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7 (1) (2) (5) (7) (14)	
SI-8	SPAM PROTECTION	SI-8 (1) (2)	
SI-10	INFORMATION INPUT VALIDATION	SI-10	
SI-11	ERROR HANDLING	SI-11	
SI-12	INFORMATION HANDLING AND RETENTION	SI-12	
SI-16	MEMORY PROTECTION	SI-16	

Table 2-13: Security Specifications - Privacy Controls

Control ID	Privacy Control Name	VA Guidance
AP	Authority and Purpose	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
AP-1	Authority to Collect	
AP-2	Purpose Specification	
AR	Accountability, Audit, and Risk Management	
AR-1	Governance and Privacy Program	
AR-2	Privacy Impact and Risk Assessment	
AR-3	Privacy Requirements for Contractors and Service Providers	
AR-4	Privacy Monitoring and Auditing	
AR-5	Privacy Awareness and Training	
AR-6	Privacy Reporting	
AR-7	Privacy-Enhanced System Design and Development	
AR-8	Accounting of Disclosures	
DI	Data Quality and Integrity	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
DI-1	Data Quality	
DI-2	Data Integrity and Data Integrity Board	
DM	Data Minimization and Retention	

Control ID	Privacy Control Name	VA Guidance
DM-1	Minimization of Personal Identification Information (PII)	Security Controls).
DM-2	Data Retention and Disposal	
DM-3	Minimization of PII used in Testing, Training, and Research	
IP	Individual Participation and Redress	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
IP-1	Consent	
IP-2	Individual Access	
IP-3	Redress	
IP-4	Complaint Management	
SE	Security	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
SE-1	Inventory of Personal Identification Information (PII)	
SE-2	Privacy Incident Response	
TR	Transparency	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
TR-1	Privacy Notice	
TR-2	System of Records Notices and Privacy Act Statements	
TR-3	Dissemination of Privacy Program Information	
UL	Use Limitation	VA Directive 6500, VA Handbook 6500, March 2015, Appendix C: (References), Appendix E: (VA System Privacy Controls), Appendix F: (VA System Security Controls).
UL-1	Internal Use	
UL-2	Information Sharing with Third Parties	

2.14. System Features

A list of system features and their descriptions will be described in the System Design Document (SDD).

2.15. Usability Specifications

Usability is a *non*-functional requirement, because in its essence, does *not* specify parts of the system functionality; but rather how that functionality is to be perceived by the user. For instance, how easily the system is learned and how efficiently it carries out user tasks.

3. Purchased Components

None identified at this time.

4. Estimation

Detail the estimation approach for the project.

If the project chooses to use function point estimation, the Function Point Estimate Workbook must be completed to support the summary information in this section. After the workbook has been completed, the data in the Application Estimate sheets must be entered in this section.

For projects that require development in multiple products, the total estimated function points are calculated as the sum of each product's estimated function points.

Instructions

- 1. Contact The VA Office of Information and Technology (OI&T) Product Development (PD) Process, Performance, and Oversight (PPO) Project Estimation Support to request an RSD-based Function Point Estimate*
- 2. Request to have a results summary returned in the format of the following table.*

Project Software Functional Size and Size-Based Effort and Duration Estimate

Application

Item	A	B	C	D	E	Total
Counted Function Points						
Estimated Scope Growth						
Estimated Size at Release						

Size-Based Effort Estimates	Labor Hours	Probability
Low-Effort Estimate – With indicated probability, project will consume no more than:		
High-Effort Estimate – With indicated probability, project will consume no more than:		

Size-Based Duration Estimates	Work Days	Probability
Low-Duration Estimate – With indicated probability, project will consume no more than:		
High-Duration Estimate -- With indicated probability, project will consume no more than:		

Figure 1: Cumulative Probability (“S-curve”) Chart

[Insert Cumulative Probability (“S-curve”) Charts here]

5. Approval Signatures

REVIEW DATE:

SCRIBE:

Signed:



Date

Deputy Director, Veterans Transportation
Program Integrated Project Team (IPT) Co- Chair

Signed:



Date

Director, Veterans Transportation Program, CBO
Business Sponsor

Signed:



Date

Software Services,
Office of Information and Technology (OI&T)

Signed:



Date

Project Manager

Appendix A: Non-Functional Requirements

The following non-functional requirements should be reviewed and accessed while developing the requirements for the project.

System Performance Reporting Requirements

(Note: Each system developed by the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T) must comply with the following mandatory requirements.)

1. Include instrumentation to measure all performance metrics specified in the Non-Functional Requirements section of the Requirements Traceability Matrix (RTM). At a minimum, systems will have the ability to measure reporting requirements for Responsiveness, Capacity, and Availability as defined in the non-functional requirements section of the RTM.
2. Make the performance measurements available to the Information Technology (IT) Performance Dashboard to enable display of “actual” system metrics to customers and IT staff.

Operational Environment Requirements

1. System response times and page load times shall be consistent with Nielsen standards (for example, My HealtheVet or HealtheVet). (Comment: There may be different expectations for an external display vs. a query. Need to address these different uses. Also indicate if this information is unknown).
2. Maintenance, including maintenance of externally-developed software incorporated into the BTSSS application(s), shall be scheduled during off-peak hours or in conjunction with relevant maintenance schedules. The business owner should provide specific requirements for establishing system maintenance windows when planned service disruptions can occur in support of periodic maintenance.
3. Information about response time degradation resulting from unscheduled system outages and other events that degrade system functionality and/or performance, shall be disseminated to the user community within 30 minutes of the occurrence. The notification shall include the information described in the current Automated Notification Reporting (ANR) template maintained by the VA Service Desk. The specific business impact must be noted in order for OI&T to provide accurate data in the service impact notice of the ANR.
4. Provide a real-time monitoring solution to report agreed/identified critical system performance parameters.
5. Critical business performance parameters shall be identified e.g., transaction speed, response time for screen display/refresh, data retrieval, etc., in a manner that data capture can occur to support metric reporting and support of the OI&T performance dashboard display. If no such performance metrics are required or provided, there will be no program specific Service Level Agreements (SLAs) created, nor shall there be any active/real-time monitoring through the OI&T Performance Dashboard to provide the business owners with any performance metrics.

6. Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance, shall be disseminated to the business-user community within a minimum of 48-hours prior to the scheduled event.

Documentation Requirements

1. The training curriculum shall state the expected training time for primary users and secondary users to become proficient at using the BTSSS application(s).
2. All training curricula, user manuals, and other training tools shall be developed/updated by the VTP/Chief Business Officer (CBO) and delivered to all levels of internal users to include the Primary Users (Beneficiary Travel Clerks and Supervisors) and the Secondary Users (Application Super Users and System Administrators). (If known, insert how much time in advance the training tools will be delivered and via what mechanism[s]; for example, 2-4 weeks in advance of the release of the enhancement through nationwide conference calls and PowerPoint presentations). The curricula shall include all aspects of the enhanced BTSSS application(s) and all changes to processes and procedures.
3. The training curriculum developed by the Program Office shall state the expected task completion time for primary and secondary users.
4. User manuals and training tools shall be developed. If they already exist, updates shall be made, as necessary, to them and they shall be delivered to all levels of users.
5. IT will provide the level of documentation required to support the system and maintain operations and continuity. Documentation shall represent minimal programmatic and lifecycle operations support documentation artifacts as defined by VA standards in ProPath and as required by the [VA Enterprise System Engineering Lifecycle and Release Management office](#) for sustained operations, maintenance, and support prior to approval by any VA change control board and released into production.

Implementation Requirements

1. Technical Help Desk support for the application, shall be provided for users to obtain assistance with the BTSSS.
2. The IT solution shall be designed to comply with the applicable approved Enterprise SLA.
3. The implementation must be complete by 30-09-2017.

Data Protection/Back-up/Archive Requirements

1. Based upon the criticality of the system, provide a back-up and data recovery process for when the system is brought off-line for maintenance or technical issues/problems.
2. Data protection measures, such as back-up intervals and redundancy shall be consistent with systems categorized as routine (30 day restoration), mission essential (72 hour restoration), or mission critical (12 hour restoration).

Business owners are required to state the mission criticality of the IT services required in order to assist the planners and developers in determining best strategies for engineering an IT solution to meet their business objectives/needs. The business owner needs to state

the criticality of the data and the impact to the business during a service disruption so appropriate technologies can be considered.

Levels for Disaster Recovery

Classification	Recovery Time Objective	Recovery Point
Objective Routine	30 day restoration	TBD
Mission Essential	72 hour restoration	24 hours
Mission Critical	12 hour restoration	2 hours

Recovery Time Objective (RTO) – RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

Maximum Tolerable Downtime (MTD) - The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

Recovery Point Objective (RPO) - The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.

Data Quality/Assurance Requirements

A monitoring process shall be provided to ensure that data is accurate and up-to-date and provides accurate alerts for malfunctions while minimizing false alarms.

User Access/Security Requirements

Ensure the proposed solution meets all Veterans Health Administration (VHA) Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see the Enterprise Requirements section of the RTM).

Usability/User Interface Requirements

Adhere to good User Interface/User Centered Design (UI/UCD) principles as outlined in the Usability Appendix of the BRD.

Conceptual Integrity

Provide standards-based messaging and middleware infrastructure needed to support both Legacy Veterans Health Information Systems Technology Architecture (VistA) and future VistA 4 deployments.

Availability

1. Maintenance window, including maintenance of externally-developed software incorporated into the VistA 4 application(s), will be by mutual agreement between OI&T and the VHA Point of Contact (POC) for the affected facility (ies). VHA will provide POCs for each facility.

2. VistA application unavailability due to an unplanned outage or planned outages that exceed the defined maintenance window will not exceed 8.76 hours per year and will not exceed 43.8 minutes per month (99.9% availability).
3. The application shall be available 24 hours a day, seven days a week, with an uptime of 99.9%.
4. All system updates and scheduled maintenance should occur between the hours of 1800 and 0600 (per local time zone), when clinical usage would be lightest.

Interoperability

1. The system shall support all recognized health system standards i.e., Health Level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR).
2. Systems must be heterogeneous and agnostic for operating systems and code bases.
3. Provide the ability to securely transfer large files (of 4-8 gigabyte) from an external source to VA systems.
4. Provide access to the system over a remote access solution.

Manageability

1. Provide Service Desk/Incident and Problem Management tracking related to maintenance events of patient care systems with priority over non-patient care systems.
2. Provide data related to maintenance events, both routine and exceptional, including key metadata:
 - Predicted routine work
 - Occurrences where maintenance is completed, including restart from down time
 - Identity of the organization performing maintenance
 - User performing maintenance (if available)
 - Identity of the system
 - Date/time, physical location
 - Systems impacted
 - Does it affect patient care
 - Non-urgent or emergent
3. Provide audit capabilities for system access and usage with settings that are configurable to support internal and external audits based on Federal and VHA mandates.
4. The system must comply with VA Directive 6300 Records and Information Management and with VHA Records Control Schedule (RCS) 10-1, in general and specifically with Electronic Final Version of Health Record: Destroy/Delete 75 years after last episode of patient care, or longer (if specified).

Performance

1. Provide an Infobutton Query Responder on all platforms with a response time of less than .5 seconds.

2. The system shall recognize, report, and retransmit data lost, with less than 0-1% chance of incomplete patient records.
3. Provide patient data (for data within the system) transactions (e.g., capture, search, request for data) within .5 seconds.
4. Mouse or key-based user interface (UI) controls, e.g., menus, checkboxes shall provide instantaneous responsiveness (<90ms).
5. Part-screen refreshes after user action shall complete within a pro-rated interval between 200 ms and 1200 ms times a percentage of the screen area being refreshed. For example, a component 10% of the screen area would refresh in $(1200 - 200) * 0.10 + 200 = 300$ ms.

Reliability

1. Provide system reliability:
 - Threshold = 99.9%
 - Objective = 99.99% system and application
2. Provide system reliability:
 - Level 1 severity =<1 failure per month
 - Level 2 severity =<2 failures per month
 - Level 3 severity =<3 failures per month

Security

Provide management of electronic attestation of information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information.

Supportability

1. Provide alerts (that extend beyond system messages to external systems like mobile devices) for malfunctions, while preventing false alarms for local, regional, and national evaluations in real time.
2. Provide reports on performance metrics as specified in the VistA 4 Effectiveness and Value / Benefits Framework on a bi-weekly basis.
3. Provide national, regional, and local reports on performance metrics as specified in the VistA 4 Effectiveness and Value / Benefits Framework.
4. Provide performance metrics (from request for information to receipt of information on the screen) monitored by the system and system administrators so they know what the user experience is like without users having to call them and tell them the system is running very slow.
5. Provide the ability for VHA and IT staff to create standard and ad-hoc reports of usage, bandwidth, response time, login time, and other variables with a verification process for measuring the capabilities of the system.

6. Provide end-user training on how to generate the various system performance reports (e.g., in standard file formats such as Comma Separated Values [CSV], Portable Document Format [PDF], or Excel) depending on the user's needs.
7. Provide the ability to view system statistics (e.g., information on the specific network environment) and identify areas that are having issues or are beyond capacity, in near-real-time (to be quantified at a later time).
8. Technical Help Desk support for the application via instant message, online, phone, and remote desktop access support, shall be provided for users to obtain assistance 24/7.
9. The IT solution shall be designed to comply with the applicable approved Enterprise SLAs.
10. Data protection measures, such as back-up intervals and redundancy shall be consistent with systems categorized as mission critical (1hr restoration, 2hr backup recovery). Impact of system failure must be monitored on a near real time basis.
11. Provide the ability to set thresholds and notification type (e.g., email or text alerts) when alerting the user about response time degradation and unscheduled outages.
12. Disaster Recovery Plans (DRP) and Continuity of Operations Plan (COOP) will be updated and tested semi-annually to address the VistA 4 product (see National Security and Homeland Security Presidential Directive: National Continuity Policy. [NSPD-51/HSPD-20, May 9, 2007](#)).

Usability

1. Provide viewability/usability of VistA 4 applications on mobile devices.
2. User prompts and screen help shall be embedded into the system to guide use of the solution.

Documentation

1. The training curriculum shall be provided in two hours or more of training time for primary users and secondary users to become proficient at using the VistA 4 application(s).
2. All training curricula, user manuals, and other training tools shall be developed/updated by the VA Program Office and delivered to all levels of users four weeks in advance of the release of the enhancement through mediums that will best support the sharing of information to all affected staff.
3. Provide follow-up training classes tailored to VHA workflow, four weeks after the users have begun to use the system.