

**Common Security Services (CSS) Conversion
01-02-04-05-05-008**

Business Requirements Document



November 2014

Revision History

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

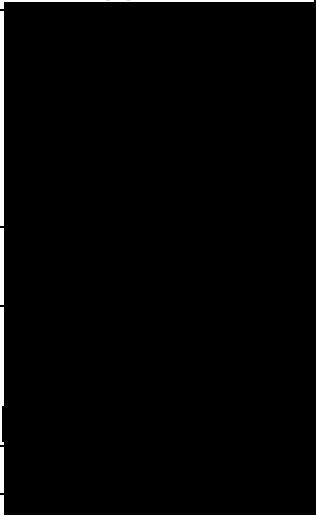
| Date | Description | Author(s) |
|------------|--|---|
| 11/13/2004 | Review and sign |  |
| 11/13/2014 | Final edit for 508 Conformance and converting to PDF for Signature | |
| 11/04/2014 | Final Draft | |
| 10/14/2014 | Initial version | |

Table of Contents

| | |
|---|-----------|
| 1. Purpose | 1 |
| 2. Overview | 1 |
| 3. Scope | 3 |
| 4. Customer and Primary Stakeholders | 4 |
| 5. Goals/Objectives and Outcome Measures | 4 |
| 6. Enterprise Need/Justification | 5 |
| 7. Business Requirements | 6 |
| 7.1. Themes, Epics (Needs), and User Narratives (Business Requirements) | 6 |
| 7.2. User Access Levels | 10 |
| 7.3. Known Interfaces and Data Sources | 10 |
| 7.4. Related Projects or Work Efforts | 11 |
| 8. Service Level Requirements | 12 |
| 8.1. Availability | 12 |
| 8.2. Capacity & Performance | 13 |
| 8.3. Interfaces and Security | 14 |
| 9. Other Considerations | 15 |
| 9.1. Alternatives | 15 |
| 9.2. Assumptions | 15 |
| 9.3. Dependencies | 15 |
| 9.4. Constraints | 16 |
| 9.5. Business Risks and Mitigation | 16 |
| Appendix A References | 17 |
| Appendix B Models | 18 |
| Appendix C Stakeholders, Users, and Workgroups | 19 |
| Stakeholders | 19 |
| Primary Stakeholder | 19 |
| Secondary Stakeholders | 19 |
| Stakeholder Support Team (BRD Development) | 19 |
| Appendix D User Interface/User Centered Design Principles | 21 |
| Appendix E Acronyms and Abbreviations | 24 |
| Appendix F Approval Signatures | 25 |
| Business Owner | 25 |
| Business Liaison | 25 |
| Customer Advocate | 25 |
| Office of Information and Technology | 25 |

1. Purpose

The Business Requirements Document (BRD) is authored by the business community for the purpose of capturing and describing the business needs of the customer/business owner. The BRD provides insight into the AS-IS and TO-BE business areas, identifying stakeholders and profiling primary and secondary user communities. It identifies what capabilities the stakeholders and the target users need and why these needs exist, providing a focused overview of the request requirements, constraints and other considerations identified. This document is a business case and does not mandate a development methodology; however, the requirements are written using agile methodology terminology. The intended audience for this document is the Office of Information and Technology (OI&T) to facilitate project planning once the project is approved and funded. These requirements are not documented at a level sufficient for development.

2. Overview

The Veterans Benefits Administration (VBA) offers a wide-variety of benefits and services to Veterans, Servicemembers, and their beneficiaries in recognition of their service to the nation. In its efforts to serve these individuals, VBA has developed applications that support their mission in the following ways:

- 1) As a database to store Veteran, Servicemember and beneficiary information
- 2) As a tool to assist in processing claims, awarding benefits and authorizing payments

In providing benefits and services, VBA gains access to personally identifiable, sensitive and Health Insurance Portability and Accountability Act (HIPAA)-protected information from individuals on a large scale and must protect this information in compliance with the Privacy Act. VBA also pays out approximately \$60 billion in benefits annually to Veterans and their dependents/survivors. Safeguarding these functions and preventing both internal and external fraud is critical to VBA's mission and ensures compliance with applicable federal laws including Federal Information Security Management Act of 2002 (FISMA) and Federal Information System Controls Audit Manual (FISCAM). Per Department of Veterans Affairs Handbook 6500, VBA is also required to put access controls in place on how users can access information systems. VBA is also required to limit access to the least privileges required to perform a particular role or function and to regularly monitor and audit that access to ensure security. To address all of these requirements VBA implemented system controls that limit access to protected information and claims processing functionality.

VBA Common Security Services (CSS) was developed to establish the necessary system controls consistent with VBA security, privacy goals and to ensure compliance with VA Handbook 6500. It is a collection of subroutines, Tuxedo application services and 32-bit Visual Basic applications including CSS Authentication, Common Security User Manager (CSUM), Common Security Employee Manager (CSEM), Common Security Application Manager (CSAM) and sensitive file checking. As a system, CSS works by instituting the following security controls:

- 1) Control of system access

- 2) Control of access to records that contain data of a sensitive nature
- 3) Review and analysis of security information

CSS plays an integral role in ensuring the security and functionality of most VBA applications, including all applications that store or read data from the VBA Corporate database, as well as many other applications that are integrated with CSS for authorization and authentication purposes only; however, it is built on Microsoft's Visual Basic 6.0 language and related technologies which have become increasingly problematic over time with its lack of full object-orientation and difficulty implementing enhancements that could have easily be done in C++ and other programming languages. A more advanced version, Visual Basic .NET offers a preferable alternative along with the following benefits:

- Supports full object orientation
- Removes the dependency on a single Integrated Development Environment (IDE) by instituting a command-line compiler
- Allows for better searching, better Intelligence and faster builds
- Integration with a decent source control system
- Resource libraries that simplify the work of encryption, XML parsing, image processing, etc.
- Enhancements will be easier to implement so the system can be continuously improved.
- Adaptability with Microsoft's other applications. Visual Basic .NET will not need to be run in XP compatibility mode.

In addition to this, VA has mandated that anyone accessing any VA information must use the framework built by the Identity and Access Management Program (IAM). To satisfy the immediate challenge of the age of the existing CSS platform and this mandate, CSS must be migrated to the IAM framework, while sustained as this effort is in progress.

VB6 applications cannot be maintained using native development tools on VBA's current desktop OS standard, Windows 7. VA was mandated by the CIO to end use of Windows XP (the current OS where Visual Basic 6 may be developed), effective September 30, 2014 as it is not a secure, supported system. Windows 7 does not have compatible development tools for the continued maintenance of VB6, making CSS effectively unsustainable until the migration to the IAM framework is complete or a stopgap is implemented. A stopgap must be completed as soon as possible as CSS is a critical dependency for VBA's applications. The inability to sustain CSS carries great risk for these applications until the migration is complete, and VBA must make all efforts possible to migrate for the long-term to the IAM platform.

VBA's Office of Business Process Integration (OBPI), the system owner for CSS, is drafting and submitting these requirements to ensure continued sustainment of VBA's security infrastructure. OBPI is responsible for overall VBA information security and serves as VBA's lead for the VA Continuous Readiness and Information Security Program (CRISP) and for the Identity and Access Management (IAM) component within the Veteran Relationship Management (VRM) Program. OBPI works with multiple affected CSS stakeholders, including VBA field staff, the Office of Information and Technology (OI&T), Office of Information Security's Field Security

Service Information Security Officers, OI&T's Service Delivery and Engineering (SD&E) Region 5 field staff at VBA regional offices and VBA's senior leadership.

3. Scope

The scope for this project has four components: 1) implementation of completed but not yet deployed CSS functionality developed as part of the VETSNET VR15 project; 2) stabilization of the VB6 CSS code by updating to an approved platform compliant with VA Technical Reference Model (TRM), 3) enhancement of the CSS Authentication application to Active Directory authentication and enabling of Personal Identity Verification (PIV) authentication via Active Directory, 4) Migration of CSS to the IAM framework.

For the purpose of the stabilization and the IAM migration, the following applications and tools must be replatformed/migrated and required modifications must be made to dependent services and data tables to enable the replatform:

- Common Security User Manager (CSUM) – This application allows management of access for users of VBA systems as well as reporting.
- Common Security Employee Manager (CSEM) – This application allows management of access for users of VBA systems, but routes this access through a workflow simplifying the access process and incorporating greater controls than the CSUM process. It does not fully replicate the abilities of CSUM.
- Common Security Application Manager (CSAM) – This application allows management of security globally across VBA applications by allowing the modification and creation of standard data (applications and functions) and by allowing the administrator to lock or unlock various VBA applications nationwide.
- CSS Authentication (CSS Authen) – This application allows the authentication of users.
- CSS Global Search (CSSGBLSRCH) – This application allows searching for CSS users across all VA stations and allows its users to quickly unlock or reset passwords for application users.
- Other tools, services and data tables – CSS has a large number of other tools, services and data tables that support a large number of other applications and functions. These tools, services and tables must be enhanced however necessary to support the replatforming.
- A complete listing of the applications and services is available in the attached spreadsheet, "CSS Application and Utility Listing". The spreadsheet is being used by the project team as a "living reference" of the various CSS applications, services and utilities as the spreadsheet may be updated to new versions subsequent to the finalization of this BRD and should not be considered a constraint on the scope of this project.

In addition to the primary replatforming effort described above, the scope of this project will include development (as needed), replatforming, testing and release of outstanding functionality and scope not delivered as part of VETSNET's VR15 project. CSS development occurred during the VR15 project, but functionality slated for VR15 Increment 4 and Increment 5 was not delivered. Defects identified during the testing process introduced scheduling issues to get them addressed while meeting the SIO release schedule. Additionally, several defects were not within the VR15 scope, in particular, defects associated with the application performance of CSEM

(which affected usability). As part of the replatform efforts, delivery of these unreleased enhancements and the elimination of outstanding significant CSS defects must be completed. The last item within scope is the enhancement of the CSS Authen application to change its authentication method to leverage the Windows Active Directory services instead of its current authentication which uses a separate CSS password and a third party tool for encryption. The CSS Authen application will need to be enhanced to not only use Active Directory, but specifically the PIV application programming interfaces (APIs) that allow authentication using the PIV card and PIV PIN. By making these changes, CSS will stay consistent with the web only component of CSS (siteminder), which uses Active Directory. CSS will also support the Homeland Security Presidential Directive 12 goal of shifting authentication to use PIV cards and two-factor authentication.

4. Customer and Primary Stakeholders

The Office of Business Process Integration (OBPI), representing the Veterans Benefits Administration (VBA), Office of Information Technology (OI&T) Office of Information Security (OIS) Field Security Service (FSS) Information Security Officers (ISO) and OI&T Service Delivery and Engineering (SD&E) Region 5 staff are the primary stakeholders for this request.

Review [Appendix C](#) for the complete list of primary and secondary stakeholders.

5. Goals/Objectives and Outcome Measures

The goal of this project is to migrate CSS to IAM and to replatform CSS to a platform where it can be sustained until that migration is complete. This migration and replatforming, along with the implementation of necessary enhancements and updates, will maintain the system's current functionality and guarantee the continued sustainment of VBA's security infrastructure. Furthermore, the replatforming and enhancement delivery will positively impact CSS users by upgrading the application's ability to respond with greater speed and efficiency to access requests as well as its eventual compliance with the IAM framework.

| Goal/Objective and Desired Outcome | Measurement | Impact |
|--------------------------------------|--|---|
| To migrate CSS to the IAM framework. | Critical functionality, as designated by the business is successfully migrated to IAM. No critical defects exist. | This will bring CSS into compliance with the Department's mandate to use IAM and allow VBA to integrate its applications into an overall cross-enterprise security framework. |

| Goal/Objective and Desired Outcome | Measurement | Impact |
|--|---|---|
| To replatform CSS successfully to a sustainable platform that can be maintained using native development tools on VBA's current desktop OS Standard, Windows 7. Windows 7 is compatible with VB.NET and the transition will expand CSS's ability to serve future maintenance needs. | -100% of existing functionality unless approved by business to be replatforming -No major or critical defects, and fewer than 50 number of minor defects | This process will affect all integrated applications that are associated with the authenticating replatform of CSS, and will complete outstanding CSS CRISP POAMs. |
| Implementation of completed but not yet released CSS functionality developed as part of the VETSNET VR15 project. | -80% of these enhancements need to be deployed successfully | These enhancements will expand the range of features in CSS, including but not limited to: user access permissions, global search functionality, and support for VBA applications like VETSNET and VBMS and VBA-wide initiatives such as National Work Queue. |
| Enhancement of the CSS Authentication application to Windows Active Directory and the PIV application programming interfaces (APIs) that will allow a user to log in via PIV card and PIV PIN. This change will allow CSS to stay consistent with the web only component of CSS (siteminder), and will also support the VA enterprise goal of shifting authentication to use PIV cards and two-factor authentication. | -100% of this feature needs to be deployed successfully -No major or minor defects | This is a critical update to the security framework that will allow users to log into CSS with an Active Directory password, their PIV card and PIV pin. This process will provide a more seamless user log-in experience, |

6. Enterprise Need/Justification

The VA Strategic Plan for FY 2014-2020 was built on the enduring principles of the VA: being people-centric, results-driven, and forward-looking. The Agency's Priority Goals (APGs) include increasing access to benefits and services for Veterans and their beneficiaries. Essential to that goal is integration within VA and our partners to provide our workforce with the skills, tools, and leadership to meet our client's needs and expectations. In evolving VA Information Technology (IT) capabilities to meet emerging customer service expectations, new and emerging IT capabilities must be delivered that provide Veterans and eligible beneficiaries, VA employees and trusted partners the ability to access authorized VA-maintained information safely and efficiently.

Inherent in these goals is recognizing the need to continually evaluate and address concurrently emerging information security challenges. Safeguarding Federal computer systems and supporting critical IT infrastructure has been an ongoing Federal concern and the VA has implemented a number of strategies to further strengthen information security. The VA Strategic Plan lists the following strategic goals:

Manage and Improve VA Operations to Deliver Seamless and Integrated Support

- Evolve VA Information Technology Capabilities to Meet Emerging Customer Service / Empowerment Expectations of Both VA Customers and Employees
- Ensure Preparedness to Provide Services and Protect People and Assets Continuously in Time of Crisis

Enhancing the VA's security framework is an essential aspect of achieving this mission. The VA must evaluate and streamline vulnerability assessment programs of VA facilities for internal and external threats and develop and implement an Insider Threat program in accordance with Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information – in order to protect classified material in the VA.

To succeed, VA must invest in VA facilities, technology, systems, programs, and business processes with forward-looking requirements. By migrating CSS to IAM and replatforming CSS to a platform that can be maintained on Windows 7 or beyond desktops, and instituting long-awaited enhancements in the application, the VA will meet its strategic goal by ensuring necessary security management, contingency planning, configuration management, and access controls for protecting VA sensitive information.

Performance Goals:

- Increase use of shared data and information
- Reduce number of redundant and legacy systems
- Increase wireless and mobile capabilities
- Work with the Department to reduce number of sensitive data loss incidents

7. Business Requirements

7.1. Themes, Epics (Needs), and User Narratives (Business Requirements)

Themes, epics, user narratives, user stories, and acceptance criteria will be captured in the Requirements Traceability Matrix (RTM). The requirements table below provides a list of the epics that are detailed in the RTM for the Common Security Services Conversion project. The RTM is stored as a separate document and can be accessed via the Requirements Traceability Link located in the New Service Request Database:

| Business Need (BN) | OWNR Number | Owner Requirement (OWNR) | Priority |
|---|-------------|---|----------|
| BN 1: Adhere to the Enterprise Level requirements within the Enterprise Requirements Repository (ERR) and as specifically addressed in Appendix D of this document. | | | |
| BN 2: Ensure IAM Compliance | | | |
| | 2.1 | CSS (including both the applications, services and other functionality listed in the attached spreadsheet and also any CSS-integrated applications), shall be migrated to the IAM security framework. | |

| Business Need (BN) | OWNR Number | Owner Requirement (OWNR) | Priority |
|---|-------------|---|----------|
| | 2.2 | Critical (defined jointly by OIT and OBPI through further requirements elaboration in Requirements Specifications Documents) CSS capabilities and/or architecture components shall be preserved. | |
| | 2.2.1 | CSS/IAM shall comply with VA Handbook 6500 Appendix F Access Controls, to include implementations approaches/system control values for VA Handbook 6500 requirements delegated to system owners. VBA shall define these implementations in subsequent requirements specification documents (RSDs). | |
| | 2.2.2 | CSS/IAM shall interface with and allow authentication and provisioning for both web-based applications and installed client applications, to include legacy Visual Basic and Benefits Delivery Network (BDN) applications. | |
| | 2.2.3 | CSS/IAM shall preserve or enhance (in accordance with modern security best practices and VBA-specific needs as specified in subsequent Requirements Specification Documents) the existing architecture surrounding VBA/Corporate Database record sensitivity and same station record access controls. | |
| | 2.2.4 | CSS/IAM shall ensure users who are Veterans or Veteran relatives will continue to be tracked, with user identities enumerated/linked with Veteran identities and will continue to have access limitations/controls consistent with current CSS operations. | |
| BN 3: Stabilize CSS for Eventual Transition to IAM | | | |
| | 3.1 | OIT shall ensure CSS can continue to be maintained/sustained (including new builds and releases, as needed to address defects, legislative mandates, security compliance) within a development environment compliant with the VA technical reference model (TRM). | High |
| | 3.1.1 | OIT shall ensure the components/applications of CSS listed in the attached spreadsheet are maintained. | High |
| | 3.1.2 | OIT shall modify any dependent services and/or data tables, or other files/integration points as needed to enable continued sustainment of CSS components referenced in 2.1.1. | High |
| | 3.1.3 | Allow CSEM, CSUM and other CSS GUI applications to be viewed at dynamic screen resolutions to include full screen/maximized view. | |
| BN 4: Application Enhancement Requirements | | | |
| | 3.1 | The application changes will be incorporated with BN 3. | |
| | 3.2 | The following application changes can be found in the attached spreadsheet, and in ClearQuest. | |
| | 3.2.1 | CSEM shall alert the supervisor and/or user when the user's temporary sensitive level is approaching expiration. (VNET CQ 00018551 and VNET CQ 00019829) | Medium |
| | 3.2.2 | CSEM shall add deleted users to CSEM history and return an indication that the user no longer exists that can be identified in the selection list by color. (VNET CQ 00018761 and VNET CQ 00019828) | Medium |

| Business Need (BN) | OWNR Number | Owner Requirement (OWNR) | Priority |
|--|-------------|--|----------|
| | 3.2.3 | CSEM shall send approval and disapproval emails to the test mailboxes assigned on the Director Approval screen in CSEM. (VNET CQ 00019626) | Medium |
| | 3.2.4 | CSEM shall allow attempts made to implement application requests and auto-generate the 8824e form without producing Oracle errors. (VNET CQ 00020339) | High |
| | 3.2.5 | CSEM shall auto-generate the 8824e with accurate information provided in the application request. (VNET CQ 00017172) | High |
| | 3.2.6 | CSEM shall update the 'Temporary Change Expires On' field on the Sensitive Access Level Request form for requests implemented via the Multi Implement Screen. (VNET CQ 00020379) | High |
| | 3.2.7 | CSS Authen shall force User IDs less than 8 characters to reset their passwords when they first gain access to the system or when the password is reset through CSUM. (VNET CQ 00020627) | High |
| | 3.2.8 | CSS Authen shall lock user accounts after three invalid password attempts. (VNET CQ 00020828) | High |
| | 3.2.9 | CSAM shall add a new application indicator to signify if an application is internal or external in the application table, and this feature will be updatable through CSAM. (VNET CQ 00019426) | Medium |
| | 3.2.10 | CSEM shall allow for access to the Virtual VA application when user access is updated via CSEM. (VNET CQ 00019119) | High |
| | 3.2.11 | CSEM shall add a new FTE indicator for employees that are exempt but includes in the station's FTE on the New User screen. (VNET CQ 00019397) | High |
| | 3.2.12 | CSUM shall add a new indicator to the database in the PERSON_SCRTY_LOG record to store the new FTE indicator for employees that are exempt but included in the station's FTE. (VNET CQ 00019396) | High |
| | 3.2.13 | CSUM shall remove invalid applications from VSOs. (VNET CQ 00020731) | High |
| | 3.2.14 | CSS shall send an email notification at 14, 7, and 1 day prior to 90 day countdown of VBA application inactivity. (VNET CQ 00020177) | Medium |
| | 3.2.15 | CSEM shall ISOs to delete inactive CSEM accounts without reactivation by IRM. (VNET CQ 00021088) | Medium |
| | 3.2.16 | CSUM shall mark the Sensitive Reason field as a required field under Sensitive File Maintenance, (Insert CQ #) | Medium |
| BN 4: Authentication Requirements | | | |
| | 4.1 | CSS/IAM shall use Windows Active Directory (including capabilities that integrate with Personal Identity Verification (PIV) cards) for authentication. | High |
| | 4.1.1 | CSS/IAM shall accept both the Windows password and the PIV pin for authentication. | |
| | 4.1.2 | CSS/IAM shall allow VBA to selectively restrict authentication using the Windows password either by station, by user, or nationally so that users may only be able to use the PIV. | |
| | 4.1.3 | CSS/IAM shall allow the user's CSS account to be locked independent of the user's Active Directory Account | |

| Business Need (BN) | OWNR Number | Owner Requirement (OWNR) | Priority |
|--|-------------|---|----------|
| | 4.1.3.1 | CSS/IAM shall automatically lock a user's CSS/IAM account after three (3) unsuccessful login attempts within a 24 hour period per VA Handbook 6500 requirements. | High |
| | 4.1.3.2 | CSS/IAM shall automatically lock a user's CSS/IAM account after thirty (30) days of inactivity. | |
| | 4..2 | CSS/IAM shall automatically end a user's session after fifteen (15) meeting of inactivity per VA Handbook 6500 requirements. | |
| | 4.3 | If a PIV card was used for authentication, CSS/IAM shall end the user's session when a PIV card is removed. | |
| BN 5: Additional Security Requirements | | | |
| | 5.1. | CSS/IAM shall (at a frequency to be determined in subsequent Requirements Specification Documents) automatically validate a user's continued employment with VA or affiliation as a contractor against designated authoritative database(s) (to be determined by analysis) and shall terminate access if a user leaves affiliation with VA. | |
| | 5.1.1 | CSS/IAM shall integrate with a VA Human Resources database (or database populated with human resources data) containing status information on employee employment or affiliate affiliation with VA. | |
| | 5.1.2 | CSS/IAM shall integrate with planned databases designed to track contractor onboarding/off-boarding. | |
| | 5.2 | CSS/IAM shall expand the existing sensitive inquiry logging and shall implement record inquiry logging for all record accesses within the Corporate infrastructure, to include long-term storage of record accesses. Per the request of VA OIG. | |
| BN 6: Security Documentation | | | |
| | 6.1 | CSS/IAM shall deliver, as part of the completed project, complete documentation on every component of the final architecture, to include completely documented interfaces, data structures, application operation and security compliance. | |
| | 6.2 | CSS/IAM shall publish and maintain (into sustainment) all necessary documentation for new project starts or newly integrating projects to interface with its security architecture and implement its security model. | |
| BN 7: Test Requirements | | | |
| | 7.1 | CSS/IAM shall allow "test" accounts to be created for non-production environments. | |
| | 7.1.1 | CSS/IAM test accounts shall allow a user in a test environment to authenticate initially using his Active Directory/PIV account and then additionally using a separate test user-ID and password combination such that a single user can access multiple test accounts for the purposes of testing different security configurations. | |
| | 7.1.2 | CSS/IAM shall automatically create test user accounts as described in 7.1.1. CSS/IAM shall allow the automatic creation of either single or multiple (minimum of 100 per transaction) accounts. | |

| Business Need (BN) | OWNR Number | Owner Requirement (OWNR) | Priority |
|--------------------|-------------|---|----------|
| | 7.1.3 | CSS/IAM shall allow access using test accounts to be enabled or disabled. | |
| | 7.1.3.1 | CSS/IAM shall default access using test accounts to be “disabled” in any test environments containing PII. Users may still authenticate using their true accounts if appropriate access is granted through the production access request process. | |
| | 7.1.3.2 | CSS/IAM shall permanently disable access using test accounts in production environments. | |

7.2. User Access Levels

Different CSS applications (CSUM, CSEM, CSAM and CSSGBLSRCH) have different user access levels. CSS will retain the existing user access levels from the current application during the replatforming effort unless a need is identified to redefine these levels during the effort in which case RSDs will be submitted to alter the levels. Long-term user access levels will be defined in the specific RSDs for IAM. For the sake of simplicity, existing user access levels will not be documented here for each of the various CSS applications.

7.3. Known Interfaces and Data Sources

This is the business community’s best understanding of known interfaces and may not be a comprehensive listing. All listed interfaces should be included in the RTM

| Name of Application | Description of current application | Interface Type | Existing Functionality | Expected Outcome |
|----------------------------|--|------------------|------------------------|--|
| Master Veteran Index (MVI) | Source of VA person identity information | Outbound | No | Demographic information will be automatically incorporated |
| PAID | Source of VA employment status | Inbound | Yes | Demographic information will be automatically incorporated |
| All VBA applications | Use the CSS suite of tools for administrating User access to all VBA corporate data. | Inbound/Outbound | Yes | Regulate access to VBA Systems and data |
| VBA Corporate Database | Database where VBA-specific claimant and claims information is stored. | Inbound/Outbound | Yes | Corporate Database connections continue to work. |
| Benefits Delivery Network | Legacy VBA application and database used to process a limited number of claims. | Inbound/Outbound | Yes | Preserve interface until BDN can be decommissioned. |

| Name of Application | Description of current application | Interface Type | Existing Functionality | Expected Outcome |
|------------------------------|--|------------------|------------------------|--|
| Benefits Enterprise Platform | Serves as security layer and messaging layer for web applications connecting to VBA Corporate Database | Inbound/Outbound | Yes | Preserve BEP connections and/or redesign BEP security with IAM transition. |

7.4. Related Projects or Work Efforts

All existing and future applications that interact with the VBA Corporate database will be dependent on the CSS suite of applications for enforcing security for applications, user roles, and sensitivity levels. The following listing are the current VBA applications that rely on CSS for security that will have to update their security controls to the newly developed CSS and IAM framework for VBA:

AWARDS (C&P)

BDN (C&P)

COVERS (C&P)

COVERS SEQ (C&P)

COWC (FINANCE)

CRMUD (EDU)

CSEM (OBPI)

CSSGBLSRCH

CSUM (CSUM Administrator & ISO Only)

EVR (C&P)

FAS (FINANCE)

FAST TRACK (C&P)

FBS (C&P)

FCMT (C&P)

FOCAS (EDU)

FTS (C&P)

LSC (LGY)

MAP-D (C&P)

MILPAY (C&P)

PIESCREATE (C&P)

PIESRESPOND (C&P)

QAWEB (VRE)

RBA (C&P)
 SHARE (C&P)
 SOC (C&P)
 SPP (C&P)
 TIMS (EDU)
 VBMS (C&P)
 VBMS-SP (C&P)
 VETSNET (C&P)
 VIRTUAL VA (C&P)
 VIERS (C&P)
 VIS (C&P/VHA)
 WEAMS (EDU)
 WEBHINQ (VHA)
 WINRS (VR&E)
 WSMS (EDU)

8. Service Level Requirements

8.1. Availability

| Service Level Requirement (SLR) Question | SLR Criteria | Description |
|---|---------------------------------------|--|
| 1. How much time should the system be available (and how much down time is acceptable due to incident [unexpected] outage)? | 99.9% (8.76 hours down time annually) | |
| 2. When should the system be available (what will be the core operating hours of the system)? | 24x7 | |
| 3. How soon should the system fully recover from an outage? (Includes Mean Time to Restore) | 2 hours | Short timeframe justified because security platform outage would limit outage to all other applications for nearly 40,000 users. |
| 4. How much data will be restored when outage is recovered? | 24 hours back | |

| Service Level Requirement (SLR) Question | SLR Criteria | Description |
|---|---|--------------------|
| 5. What time period should be considered for maintenance periods? | Coordinated installs as scheduled on the Benefits Development Calendar (typically one Saturday evening through Sunday morning every other month). | |
| 6. What standard time zone will the system operate in? | All time zones (system is located in Central Time Zone) | |

8.2. Capacity & Performance

| SLR Question | SLR Criteria | Description |
|---|---|---|
| 1. How many users will be on the system hourly? | >50,000 | All users needing access to VBA corporate data will have to utilize this system to gain access |
| 2. How many transactions will each average user perform each hour? | >500 from CSUM, CSAM, CSEM >100,000 for security infrastructure components including authentication and sensitive checks | Users will be of two types, one using other applications that use CSS for authentication and members of the security community that will use tools to manage user access. |
| 3. What are the anticipated peak user times during the day? | Other (specify) | 7 AM– 12PM ET; 1 PM – 4 PM ET Monday through Friday excluding Federal Holiday |
| 4. What is the anticipated peak transaction load (when do you think that there will be the most transactions being performed on the system) during the day? | Other (specify) | 7 – 12PM ET; 1 – 4PM ET Monday through Friday excluding Federal Holiday |
| 5. How many new users will be added in one year? | >5000 | The system manages the addition and removal of all users with access to the VBA Corporate data base. |
| 6. How many more (if any) transactions will be added in one year? | >5000 | Business Users? |

| SLR Question | SLR Criteria | Description |
|--|---|--|
| 7. What kind of information will be stored (specify average of each kind per month)? | Everything VBA has about a Veteran and their dependents | PII, demographic, health and other data about Veterans and their dependents; a variety of documents of varying sizes |
| 8. What kind of search capacity is required? | Heavy (greater than 1,000 per hour) | Functionality to search is built in to a large number of the applications that use CSS for authentication; additionally the CSS User management tools allow for the searching for specific employees |
| 9. What type of system(s) is/are required? | All: Local (regional) Intranet (All VA) Internet (public) | As CSS controls access to all VBA Corporate data all other systems from local to nationally deployed including those providing data access through the Intranet and the Internet will be utilizing this. |
| 10. Is there a need for heavy application reporting? If yes, when? | End of day End of month End of quarter Other (specify) | There are a lot of different reports run at different times for different audiences with different requirements. |

8.3. Interfaces and Security

| SLR Question | SLR Criteria | Description |
|--|--------------|--|
| 1. Does this system interact with other existing systems? | Yes | All systems that access VBA Corporate Data must come through CSS in order to get access to the data. |
| 2. Will this system require additional monitoring for Information Technology system metrics? | Yes | As this system is a gate keeper its performance is of the utmost importance. |

| SLR Question | SLR Criteria | Description |
|---|--------------------------|--|
| 3. Will this system contain personally identifiable information, Protected Health Information, Health Insurance Portability and Accountability Act (HIPAA) information, or other confidential/regulated data? | Yes | |
| 4. Who will be the anticipated users of this system? | Regional VA Public | Anyone with a need to access VBA Corporate data. |

9. Other Considerations

9.1. Alternatives

There is no acceptable alternative than the migration of CSS to IAM as the system is not sustainable in its current state or platform. The replatforming and subsequent transfer to IAM reduces the risk to VBA's security, and is necessary due to the system's current outdated dependencies on Windows XP. As Windows XP is not a supported system and poses a great deal of risk if the system is compromised, CSS, an essential system upon which all VBA applications rely, must be migrated off of it as mandated by the VA CIO.

9.2. Assumptions

- IAM will be able to address via configuration or enhancement, all of VBA's security requirements.
- Applications integrated with CSS will have sufficient funds and sustainment support to address interface changes introduced as part of either the CSS sustainment work or migration to IAM.
- VBA BEP, BGS, Tuxedo and VBA Corporate architecture developers will make modifications as necessary to support any changes introduced by the CSS work to existing security models.
- IAM Provisioning/access management application(s) is 508 compliant.
- IAM provisioning/access management application(s) are compliant with current and will kept in compliance with future VBA desktop image standards for web browsers (i.e. IE 11 and on).

9.3. Dependencies

- Availability of resources with sufficient knowledge of existing CSS applications, services and data.
- Availability of resources for web service and database development.
- Availability of IAM resources

- Schedule dependent upon integrating/connected applications and their major release scopes (e.g. VBMS, VRM) and ability to address, deploy changes to security.
- Changes to existing security requirements/handbooks/implementations within and without VA (e.g. changes to VA Handbook 6500, NIST, etc.)

9.4. Constraints

- Final products must be compliant with VA Handbook 6500 requirements and VA's technical reference model.
- Key resources with systems knowledge are retiring before end CY 2015.
- Existing systems cannot be sustained and VBA will incur significant security risk until initial migration is completed.
- Concurrent efforts for both interim and final solutions must be supported to transition multiple VBA applications.
- Even in the midst of development, sustainment activities and other changes to support releases of other VBA applications must be supported.

9.5. Business Risks and Mitigation

| Business Risks | Mitigation |
|---|--|
| There may be insufficient funding to support migration to IAM. | Submit timely UFRs and escalate priority with senior leadership. |
| If schedule is not met, VBA's unsustainable security applications are either at greater risk for security breaches, or at greater risk of disabling access to VBA systems. | Work to immediately replatform CSS to a better long-term sustainment posture. |
| As CSS is a critical support system, key projects may request security changes/enhancements to achieve high priority organizational objectives that may divert from initial | Work with VETSNET team to ensure sustainment support is adequate to prevent diversion of development resources. |
| Software developed is non-compliant with security requirements. | Work closely with OIS and ISOs to ensure compliance of requirements and solutions are validated at every step of the development process. |
| CSS replatform will need to be 508 compliant, but funds may not be available to enable functionality. | Contact VETSNET PM and 508 Compliance Office to identify alternatives available to ensure CSS replatform meets compliance standards or investigate waiver if not pending IAM implementation. |

Appendix A References

- Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)
- Federal Information System Controls Audit Manual (FISCAM)
[REDACTED]
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- VA Directive 6500, Managing Information Security Risk: VA Information Security Program;
- VA Handbook 6500 – Risk Management Framework for VA Information Systems
[REDACTED] [v](#) [REDACTED]
-

Appendix B Models

Appendix C Stakeholders, Users, and Workgroups

Stakeholders

Primary Stakeholder

Veterans Benefits Administration (VBA)

Office of Business Process Integration (OBPI)

Office of Information Technology (OI&T)

Office of Information Security (OIS) Field Security Service (FSS)

Information Security Officers (ISO)

OI&T Service Delivery and Engineering (SD&E) Region 5

Secondary Stakeholders

- VBA Office of Field Operations
- All VBA Application Users
- VBA Lines of Business/System Owners
 - Compensation Service
 - Pension and Fiduciary Service
 - Insurance Service
 - Loan Guaranty Service
 - Benefits Assistance Service
 - Vocational Rehabilitation and Employment Service
 - Education Service
- Veterans

Stakeholder Support Team (BRD Development)

| Type of Stakeholder | Description | Responsibilities |
|---------------------|---|--|
| Requester | ██████████ Office of Business Process Integration | Submitted request. Submits business requirements. Monitors progress of request. Contributes to BRD development. |
| Endorser | ██████████ of Business Process Integration | Endorsed this request. Provides strategic direction to the program. Elicits executive support and funding. Monitors the progress and time lines. |

| Type of Stakeholder | Description | Responsibilities |
|---|-------------|---|
| Business Owner(s)/Program Office(s) | | Provides final approval of BRD with sign-off authority. Provides strategic direction to the program. Elicits executive support and funding. Monitors the progress and time lines. |
| Business Subject Matter Expert(s) (SME) | | Provide background on current system and processes. Describe features of current systems, including known problems. Identify features of enhancement. |
| Technical SME(s) | | Provide technical background information about the current software and requested enhancements and the "to-be" framework being created by IAM. |
| User SME(s) | | Ensure that the enhancements will account for current business processes and existing software capabilities. |
| Security Requirements SME(s) | | Responsible for determining and providing guidance on compliance with HIPAA, Privacy Act, FISMA, FISCAM. |
| Service Coordination SME(s) | | Responsible for ensuring all aspects of non-functional requirements have been accurately recorded for this request. |
| Business Liaison Staff | | Serve as the liaison between the Program Office (Business Owner) and Product Development throughout the lifecycle. |

| Type of Stakeholder | Description | Responsibilities |
|-------------------------------------|---------------------|---|
| Requirements Analyst(s) | • • • | Responsible for working with all stakeholders to ensure the business requirements have been accurately recorded for this request. |
| Project Manager | • | Manage the day to day details of the project to completion. |
| Program Manager | • | Responsible for the Program under which this conversion is taking place. |
| OIT Officer of Responsibility (ORR) | • | Ultimate IT responsible official for the completion and deliver of this project. |

Appendix D User Centered Design Principles

User Experience encompasses direct and indirect interactions between the user and the system. Improving usability over the prior version is a key requirement for this application. The International Organization for Standardization (ISO) defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use” (1998).

For an optimal user experience the system must meet the requirements outlined in this section, which involve attributes of the application and the process required to achieve them.

In order to improve usability of VA-developed or purchased applications, the following actions are required:

- In accordance with the Office of the National Coordinator for Health Information Technology’s Meaningful Use Stage 2 final ruling, employ an industry recognized User Centered Design (UCD) process. The methods for UCD are well defined in documents and requirements such as ISO 9241-11, ISO 13407, ISO 16982, National Institute of Standards and Technology Interagency Report 7741, ISO/International Electrochemical Commission 62366, and ISO 9241-210. Developers will choose their UCD approach; one or more specific UCD processes will not be prescribed.
- Adhere to an industry recognized User Interface (UI) Best Practices Guideline or Style Guide. For example, first follow UI guidelines for the development platform. In instances where platform guidelines are not available, adhere to VA’s Best Practices Guidelines/Style Guide.

- Inform requirements and designs with detailed human factors work products that have been/will be completed for the specific project. Examples of specific human factors activities might include heuristic evaluations, site visits, interviews, application-specific design guides, and usability testing on existing systems or prototypes.

A sound UCD and development process based on human factors should include the following activities:

- Understanding of the users, the users' tasks, and the users' environments
- Review of similar or competitive systems to inform requirements and design
- Heuristic evaluation of prior versions, prototypes, or baseline applications, if applicable
- Iterative design and formative usability testing (formative usability testing is used to discover usability problems during the design and development process)
- User risk analysis
- Summative validation usability testing (summative usability testing is used to quantify and validate usability of a product with measures of effectiveness, efficiency, user perceptions, etc.)

To demonstrate high usability, the application should be:

- Intuitive and easy to learn, with minimal training
- Effective by allowing users to successfully complete tasks
- Efficient by allowing users to complete their work in a manner consistent with clinical practice and workflow
- Perceived to have high usability, as demonstrated by appropriate survey measures
- Designed to aid users in meeting task goals without being an additional burden

The system must be reliable and enable user trust by providing:

- Stable and reliable performance
- Accurate data
- Display of all data that is available in native or interfaced systems and intended to be available in the application
- Accessible information related to the source of data

The application should include a modern Graphical User Interface that allows the user to view data from multiple sources and include:

- Integrated display of structured and unstructured data
- Rich data visualization and graphical display of data
- Ability to switch between tabular and graphical data views
- Ability to interact with displayed data to obtain additional details related to the data and source of the data
- User customizable components and settings

The application must provide for advanced and up-to-date searching, to include:

- Fast search functionality with auto-complete and real-time display of matched results during typing
- Search history

The application must provide for advanced filtering capabilities, to include:

- Filtering of data tables, lists, and grids
- Filtering of search results

The application design should be modified to:

- Address the specific findings from a human factors heuristic evaluation conducted on the prior version of the application
- Address the specific findings reported from field use of the prior version
- Address the specific findings reported from usability testing of the prior version or relevant prototypes

Appendix E Acronyms and Abbreviations

| Term | Definition |
|-----------|--|
| • BDN | Benefits Delivery Network |
| • BGS | Benefits Gateway Services |
| • BRD | Business Requirements Document |
| • CRISP | Continuous Readiness in Information Security Program |
| • CSAM | Common Security Application Manager |
| • CSEM | Common Security Employee Manager |
| • CSS | Common Security Services |
| • CSUM | Common Security User Manager |
| • FISCAM | Federal Information System Controls Audit Manual |
| • FISMA | Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) |
| • FSS | Field Security Service |
| • HIPAA | Health Insurance Portability and Accountability Act |
| • IAM | Identity and Access Management program |
| • ISO | International Organization for Standardization or Information Security Officer |
| • NSR | New Service Request |
| • OBPI | Office of Business Process Integration |
| • OI&T | Office of Information and Technology |
| • OIS | Office of Information Security |
| • PIV | Personal Identify Verification |
| • RTM | Requirements Traceability Matrix |
| • SLR | Service Level Requirements |
| • SME | Subject Matter Expert |
| • TRM | Technical Reference Model |
| • UCD | User Centered Design |
| • UI | User Interface |
| • VA | Department of Veterans Affairs |
| • VBA | Veterans Benefits Administration |
| • VETSNET | Veterans Services Network |

Appendix F Approval Signatures

Business Owner

The requirements defined in this document are the high level business requirements necessary to meet the strategic goals and operational plans of the Office of Business Process Integration. Further elaboration to these requirements will be done in more detailed artifacts.

Signifies that the customer approves the documented requirements, that they adequately represent the customers desired needs, and that the customer agrees with the defined scope.

Signed:

_____, Director, Office of Business Process Integration Date

Business Liaison

Signifies appropriate identification and engagement of necessary stakeholders and the confirmation and commitment to quality assurance and communication of business requirements to meet stakeholder expectations.

Signed:

_____, Office of Business Process Integration Date

Customer Advocate

Confirms that the request merits consideration and review by the Business Intake Review Board.

Signed:

_____, Benefits Customer Advocate Date

Additional signature for out-of-cycle requests processed through the Business Intake Review Board: Deputy Chief Officer for Health Systems (VHA)
Executive Customer Advocate Corporate
Executive Customer Advocate Benefits and Cemetery

Office of Information and Technology

Indicates agreement that the requirements have been received, are clear, understandable, and are documented sufficiently to facilitate project planning when the project is approved and funded.

It is understood that negotiations may need to occur with the Business Owner during project planning as a result of technical reviews and feasibility.

Signed:

_____, Program Manager, Veterans Relationship Management Program Date