

# V&V Secure Design Review Validation Request Form

(VA Office of Information Security (OIS) *Secure Design Review Standard Operating Procedures (SOP)* effective 24 October 2016

This form must be used for **ALL** VA applications for Verification and Validation (V&V) secure design review validation requests. You **MUST** complete **ALL** questions that are stated to be mandatory request information unless otherwise identified on this form.

For all applications, you must:

- complete this form (*V&V Secure Design Review Validation Request Form*)
- provide all prerequisites identified for the desired type of review according to the Secure Design Review SOP
- submit this form by following [current VA Software Assurance Request Procedures](#)

Attach extra pages if there is insufficient space on this form.

For more information about secure code reviews performed at the VA, see the *OIS Secure Design Review SOP* which can be downloaded from the following

location: <https://wiki.mobilehealth.va.gov/display/OISSWA/Public+Document+Library>

## Notes for completing this form

- Section 2.3.2 of the *OIS Secure Design Review SOP* defines V&V validation request prerequisites.

## Additional instructions for application request details

Desired start and completion dates are for VA Software Assurance Program Office planning purposes only. They do not guarantee a request will begin or complete by the desired date.

## Additional instructions for question 1 “What type of review is being requested”?

- To request a location to upload file follow the procedures for registering an application on: <https://wiki.mobilehealth.va.gov/display/OISSWA/Frequently+Asked+Questions>

### Mandatory request information

### Application developer information

Application information

Name	
Version	

Component or integration information

Name	
Description	

Organization/Government primary POC

Name	
Phone	
Email	

Application technical POC (Developer Contact)

Name	
Phone	
Email	

Primary programming language(s) used in development

Check all that apply:

- |                                      |  |                                   |
|--------------------------------------|--|-----------------------------------|
| <input type="checkbox"/> ASP.NET     | <input type="checkbox"/> Java              | <input type="checkbox"/> HTML     |
| <input type="checkbox"/> Classic ASP | <input type="checkbox"/> JavaScript / AJAX | <input type="checkbox"/> TSQL     |
| <input type="checkbox"/> C           | <input type="checkbox"/> JSP               | <input type="checkbox"/> VB.NET   |
| <input type="checkbox"/> C++         | <input type="checkbox"/> MUMPS             | <input type="checkbox"/> VB6      |
| <input type="checkbox"/> C#          | <input type="checkbox"/> Objective-C       | <input type="checkbox"/> VBScript |
| <input type="checkbox"/> COBOL       | <input type="checkbox"/> PHP               | <input type="checkbox"/> XML      |
| <input type="checkbox"/> ColdFusion  | <input type="checkbox"/> PLSQL             | <input type="checkbox"/> Other    |

Desired start date for review

Desired completion date for review

### 1. V&V secure design review validation request checklist

- The Microsoft Threat Modeling file has been uploaded.
- Documentation containing lists of technologies/libraries utilized has been uploaded.
- Documentation containing sequence diagrams has been uploaded.
- Documentation containing deployment diagrams has been uploaded.
- Documentation containing lists of application interfaces and services utilized has been uploaded.
- Documentation any additional supporting documentation has been uploaded.
- Documentation containing readme file that explains where to find each of the above items within the provided documentation has been uploaded.
- All threats have been analysed in the Microsoft Threat Modeling file. All threats must be analyzed. All mitigation descriptions must include documentation references, and referenced documentation must additionally be provided. If a finding is a false positive, it has been analysed as "Not Applicable," with comments added to the Microsoft Threat Modeling file stating the reason it is considered a false positive.
- All model errors reported by Microsoft Threat Modeling have been fixed or addressed. Any errors can be seen in the Design view.
- The most recent version of Microsoft Threat Modeling was used to develop the application threat model.
- Custom rule file(s) (HP Fortify SCA ".xml" rulepack file(s)) (if any) have been uploaded.
- Provide a brief description of the security libraries and frameworks that have been used.

### 2. What are the known compliance obligations for the application? (Non-mandatory request information)

- FISMA (Federal Information Security Management Act)
- GLBA (Gramm-Leach-Bliley Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI (Payment Card Industry Data Security Standard)
- SOX (Sarbanes-Oxley Act)
- None (There are no known legal compliance obligations)
- Other \_\_\_\_\_

**3. Additional application information (Non-mandatory request information)**

Provide a brief summary of the application?  
What are some typical user transactions?

Describe the architecture of the application.

Describe the interfaces used to access the application.

If application is divided into modules or sub-applications, provide short description of each and pertinent information about each (Approx size, user roles supported, languages used, additional authentication required, etc.)

What is the level of confidentiality of the data handled by the application?

How important is integrity for the data handled by the application?

How important is availability for the application?

What is the relative risk of the application to the organization?

What is the most important / sensitive information stored in the application?

- Public Data - Is intended for external release or for use by non-employees. This data type can be disclosed to anyone without exception or consequence.
- Internal Data - Is widely available to employees during the normal course of business, but is kept within an organization's control and may not be otherwise disclosed without authorization.
- Confidential Data - Information that, if compromised, may have an adverse material impact on the organization, its customers, business partners, vendors, or employees. Information with this classification is very sensitive and is to be disseminated only to groups or individuals with a legitimate business "need to know."
- Restricted Data - Is statutorily protected and considered Confidential. Restricted data may substantially harm the organization's reputation or cause severe financial, legal, or regulatory damage to the organization, its customers, business partners, vendors, or employees if it is disclosed to anyone other than those individuals who are authorized to access or see it.
- Unknown Data - Interacts with data of an unknown classification type. Data of this type should be assumed to at least be Restricted.
- Account Access - Stores credentials or security identification codes used for system access. Information of this type is typically classified as Confidential

- Account Behavior - Stores description of baseline login behavior. Information of this type is typically classified as Public.
- Third-Party Confidential (e.g. under NDA) - Stores information provided by business partner to facilitate collaboration. Information of this type is typically classified as Confidential.
- Customer Personally Identifiable - Stores customer information defined by privacy laws as personally identifiable (including Credit Card information). Information of this type is typically classified as Restricted.
- Customer Confidential (not personally identifiable) - Stores customer information other than that defined by privacy laws as personally identifiable. Information of this type is typically classified as Confidential.
- Employee Compensation - Stores payroll, tax, and compensation algorithms associated with employee identification information. Information of this type is typically classified as Confidential.
- Deal Unannounced - Stores business partner negotiations and corresponding strategies whether by firm or on behalf of client. Information of this type is typically classified as Confidential.
- Proprietary Trade Secret Source Code - Stores programs or configurations used to run proprietary systems. Information of this type is typically classified as Restricted.
- Business Trade Secrets - Stores data with respect to business strategy and product delivery. Information of this type is typically classified as Confidential.
- Business Operational - Stores data with respect to internal business operations, IT, inventory, workers, or process. Information of this type is typically classified as Internal.
- Employee Personally Identifiable - Stores employee information defined by privacy laws as personally identifiable. Information of this type is typically classified as Confidential.
- Public Customer Information - Stores marketing-related customer information not covered by privacy regulation. Information of this type is typically classified as Public.
- Public Government Information - Stores information published by business or available through authorized business process. Information of this type is typically classified as Public.
- Transactions in Progress - Stores details concerning transitions prior to being made part of public record. Information of this type is typically classified as Confidential.
- Wide Distribution Nonpublic - Stores publications, including software, covered via copyright or license agreements. Information of this type is typically classified as Internal.

What type(s) of authentication are used or supported by application?

- Windows Active Directory
- Form Based Username/Password
- HTTP Basic Authentication
- HTTP Digest Authentication

- Client Certificate
- NTLM
- VAMF (VA Mobile Framework)
- OAUTH
- Other \_\_\_\_\_

What is the project's classification (direct consumer(s) of the application)?

- Government-wide - Support for government administrative functions
- Market Strategy - Marketing and pricing
- Product - Product delivery and confirmation
- Publishing - Non-product media or other material distribution
- Research - Conduct and/or distribute research
- Regulatory - Regulatory data gathering and reporting
- Risk Management - Government and counterparty analysis
- Sales - Customer relationship management and transaction processing
- Services - Customer support and service delivery improvement systems
- Other \_\_\_\_\_

What is the level of access required to interact with the application?

- Internal Network Access Required Interaction can only occur when connected to the internal VA network
- External Public Network Access Required Interaction can only occur from an untrusted public network (e.g. the public internet)
- Secured Connection with Business Partners Interaction can only occur through a secured connection from a business partner
- Console Access Interaction can only occur through a console connected directly to the computer hosting the application (e.g. serial terminal access)

How is data transmitted to/from the application?

What type of users will be accessing this application?

- Check here if users are VA Employees, Contractors, Volunteers, and other acting on behalf of VA
- Check here if users are the Public (Citizens, Veterans, Businesses, and others NOT acting on behalf of the VA)
- Check here if users are Other VA Applications

What is the average number of users for the application per day?

Describe the user types and roles that exist within the application? (e.g. user, administrator,

auditor, helpdesk, etc.)

Does the application provide self-registration of user accounts? Is admin approval of registered accounts required?

Please attach application Flow/Usage diagrams or design documentation if available

Select One checkbox for how the application should be analyzed.

- High Risk Application - Requires Read and/or write access to VA sensitive resources
- Medium Risk Application - Requires Write access to VA resources.
- Low Risk Application - Requires Read only access to VA resources
- Very Low Risk Application - Does not utilize VA resources

What is the most damaging or dangerous action that could occur in the application? e.g. read only users can modify data, users can view other users' credit card information, etc.

For server side applications/components, what platform will the application be deployed to?

- Linux
- Windows
- Platform Neutral
- Other \_\_\_\_\_

For client side applications/components which platforms will the app support?

- Desktop Browser
- Desktop Client
- Apple Browser
- Apple Native
- Android Browser
- Android Native
- Microsoft Mobile Browser
- Microsoft Mobile Native
- Other \_\_\_\_\_

For mobile apps, select the entitlements that the app will need access to

- Access Camera
- Access GPS
- Access Calendar
- Access Contacts
- Access Reminders
- Access Photos
- Access Internet

<input type="checkbox"/> Store Data Locally
<input type="checkbox"/> Other _____

---

**FOR OFFICE USE ONLY**

Date received

NSD ticket number

JIRA ticket number

Uploaded code location