

# V&V Quality Code Review Validation Request Form

(VA Office of Information Security (OIS) *Quality Code Review Standard Operating Procedures (SOP)* effective 11 January 2018)

This form must be used for **ALL** VA applications for Verification and Validation (V&V) quality code 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 Quality Code Review Validation Request Form*)
- provide all prerequisites identified for the desired type of review according to the Quality Code Review SOP
- submit this form by following the procedures on the VA Software Assurance Support Site <https://wiki.mobilehealth.va.gov/display/OISSWA/Frequently+Asked+Questions>

For more information about secure code reviews performed at the VA, see the *OIS Quality Code 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 2.3.1 of the *OIS Quality Code 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 scan file(s) and source code follow the procedures for requesting directories on: <https://wiki.mobilehealth.va.gov/display/OISSWA/Frequently+Asked+Questions>
- To provide McCabe complexity values for table B, SourceMonitor (<http://www.campwoodsw.com/>) can be used to quickly analyze the lines of code and the McCabe Cyclometric complexity values for your source code. SourceMonitor measures metrics for source code written in C++, C, C#, VB.NET, Java, Delphi, Visual Basic (VB6) and HTML
- For a .NET application or any application built using Visual Studio, the following is required: the source code for the application (.cs files), as well as all libraries, frameworks, dll's, xml configuration files, build files and any other 3rd party dependencies
  - Provide a zip file containing each Visual Studio solution's top level directory and all subdirectories. For an ASP.NET application, with C# source files, this includes all .sln, .suo, .csproj, .cs, .aspx, .ascx, .asax, .asp, .config, .xml, .resx, .settings, .dll, .exe, .pdb, .txt, .cache, etc. files included in the Visual Studio solution and generated by Visual Studio.
  - Any libraries (external .dll files) referenced by the solution, which are not included in the Visual Studio solution directory hierarchy must also be included
- For a Java application, the following is required: the source code for the application (.java files), the build script used to build the class, jar, and any executable files produced. This includes all of the Ant (build.xml) or Maven (pom.xml) build scripts for the Ant or Maven projects, as well as all libraries, frameworks, .jar files, xml configuration files, properties files, and any other 3rd party dependencies.
  - Provide a zip file containing everything in the project's Eclipse directory and workspace directory structures (or directory structure for the IDE used to develop and build the application).
  - For Eclipse, provide the .metadata directory, or specific instructions for loading the workspace and projects into Eclipse, so that all projects can be compiled and built successfully

**Mandatory request information****Application developer information**

Application information

Name	
Version	

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    |

Fortify build tool(s) used

(For more information regarding build tools, please refer to the following Technical Note:

Note: <http://go.va.gov/ai8p>; please make sure that the correct tool was used before requesting a quality code review validation)

- 
- Command-line tools

- 
- Scan Wizard

- 
- IDE Plugins

- 
- Build Environment Integration

- 
- Audit Workbench

Please enter the command used or the options passed to Fortify for the translation phase:

Were scripts used with any of the above-selected Fortify build tools?

- 
- Yes\*

- 
- No

\*If "Yes", please upload the scripts to the share along with the other required submission materials.

Desired start date for review

Desired completion date for review

## 1. V&V quality code review validation request checklist

- The complete and buildable application source code (to use when reviewing scan result file) has been uploaded.
- The source code uploaded matches the source code scanned with Fortify. The version of all source code files uploaded is the same as the code scanned with Fortify and all files provided have been scanned with Fortify.
- Scan result file(s) (HP Fortify SCA ".fpr" file(s)) have been uploaded.
- All findings reported by Fortify have been analysed in the FPR file(s). All code quality findings must be fixed. If a finding is a false positive, it has been analysed as "Not an Issue," with comments added to the FPR stating the reason it is considered a false positive.
- All errors/exceptions/warnings reported by Fortify during the scan(s) have been fixed or addressed. Any errors/exceptions/warnings reported by Fortify can be seen in Audit Workbench. Go to the "Project Summary," "Analysis Information" tab, "Warnings" sub-tab.
- The most recent version of Fortify, and the complete, most recent set of the Fortify rulepacks were used when scanning the code.
- Custom rule file(s) (HP Fortify SCA ".xml" rulepack file(s)) (if any) have been uploaded.
- Provide a brief description of the frameworks that have been used.

- Source lines of code (SLOC): \_\_\_\_\_
- Number of source code and configuration files: \_\_\_\_\_
- Number of classes, if applicable: \_\_\_\_\_

## 2. Additional application information (Non-mandatory request information)

Has a source code analysis/scan been performed against the application previously? If so, please provide any details available about the scan.

What build tools are used? E.g. Ant or Maven for Java; Version of Microsoft Visual Studio for .NET

Is this a new or legacy application? If it is new, will multiple code reviews be required during the software development lifecycle, or prior to multiple releases of the application?

What is the development strategy used for the application?

Is software architecture and/or design documentation available?

Can all libraries, frameworks, dll's, xml configuration files, make, Ant or Maven build files and any other 3<sup>rd</sup> party dependencies be provided with the source code?

Is a version control system used to manage the application source code? If yes, what VCS software tool is being used?

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, etc.)

How important is availability for the application?

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 \_\_\_\_\_

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?

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

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 OFFICE USE ONLY**

Date received

NSD ticket number

JIRA ticket number

Uploaded code location