V&V Code Review Validation Request Form

(VA Office of Information Security (OIS) Software Assurance Program Form effective 22 July 2019)

This form must be used for **ALL** VA applications for Verification and Validation (V&V) 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 Code Review Validation Request Form)*

- submit this form by following the procedures on the VA Software Assurance Support Site
  https://wiki.mobilehealth.va.gov/display/OISSWA/Frequently+Asked+Questions

Notes for completing this form

- Fortify SCA validation request packages must contain the following items:
    - V&V secure code review request form that has been filled out,
    - Complete and buildable application source code (to use when reviewing scan result file),
    - 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,
    - Static analysis tool scan result file (HP Fortify SCA ".fpr" extension file),
    - All findings reported by Fortify have been analyzed in the FPR file(s). All critical and high findings must be fixed. If a finding is a false positive, it has been analyzed 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.
    - Static analysis tool custom rule file(s) (if any) (HP Fortify SCA ".xml" rulepack file(s))
- Contact the VA Software Assurance Program Office at OISSwAServiceRequests@va.gov for prerequisites for other allowed code review tools.

Additional instructions for application request details

Desired start and completion dates are for VA Software Assurance Program Office planning purposes only. They 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 registering applications 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.

- o 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).
- o 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:

- ☐ ASP.NET
- ☐ Classic ASP
- ☐ C
- ☐ C++
- ☐ C#
- ☐ COBOL
- ☐ ColdFusion
- ☐ Java
- ☐ JavaScript / AJAX
- ☐ JSP
- ☐ MUMPS
- ☐ Objective-C
- ☐ PHP
- ☐ PLSQL
- ☐ HTML
- ☐ TSQL
- ☐ VB.NET
- ☐ VB6
- ☐ VBScript
- ☐ XML
- ☐ Other

Scan tool & scan build tool(s) used

(Please make sure that the correct tool was used before requesting a secure code review validation)

If using Fortify SCA, check all that apply:

- ☐ Command-line tools
- ☐ Scan Wizard
- ☐ IDE Plugins
- ☐ Build Environment Integration
- ☐ Audit Workbench

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

Were scripts used with any of the above-selected 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 secure 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 the code review tool. The version of all source code files uploaded is the same as the code scanned with the tool and all files provided have been scanned with the tool.

☐ Scan result file(s) (e.g. Fortify SCA ".fpr" file(s)) have been uploaded.

☐ All findings reported by the tool have been analysed in the scan file(s). All critical and high findings must be fixed. If a finding is a false positive, it has been analysed as "Not an Issue," with comments added to the scan file stating the reason it is considered a false positive.

☐ All errors/exceptions/warnings reported by the code review tool during the scan(s) have been fixed or addressed. Any errors/exceptions/warnings reported by the tool can be seen in e.g. for Fortify, the Audit Workbench, on the "Project Summary," "Analysis Information" tab, "Warnings" sub-tab.

☐ The most recent version of the code review tool and the complete, most recent set of the its rulepacks (if applicable) were used when scanning the code.

☐ Custom rule file(s) (e.g. 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.

☐ Source lines of code (SLOC): _____

☐ Number of source code and configuration files: _____

☐ Number of classes, if applicable: _____

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)

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?	
Are security requirements defined and available for the application?	
Are misuse and abuse cases defined and available for the application?	
Is software architecture and/or design documentation available?	
Is a threat model available for the application? If no, does a threat assessment need to be performed?	
Can all libraries, frameworks, dll's, xml configuration files, make, Ant or Maven build files and any other 3rd 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?	
Does an Architectural Risk Assessment, which identifies architectural flaws with security implications, need to be performed?	
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 classifications 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
- [ ] Store Data Locally
- [ ] Other _____

FOR OFFICE USE ONLY

Date received

Ticket number

Uploaded code location