

OFFICE OF
INFORMATION
SECURITY

Secure Code Review
Standard Operating Procedures

JUNE 2014



Office of Information Security

Table of Contents

| | |
|---|---|
| 1. Introduction | 1 |
| 1.1 Document Audience..... | 1 |
| 1.2 Secure Code Review Overview | 2 |
| 1.3 V&V Secure Code Reviews | 2 |
| 2. V&V Secure Code Reviews | 3 |
| 2.1 Roles and Responsibilities..... | 3 |
| 2.2 Process Overview | 4 |
| 2.2.1 Activities During Development | 4 |
| 2.2.2 Activities During A&A Process..... | 4 |
| 2.2.3 Activities During Validation | 5 |
| 2.3 Validation Process..... | 5 |
| 2.3.1 Prerequisites..... | 5 |
| 2.3.2 Scheduling | 6 |
| 2.3.3 Deliverables..... | 6 |
| Appendix A – Resources..... | 7 |
| Appendix B – IV&V Incident Response Secure Code Reviews | 8 |

Table of Figures

| | |
|---|---|
| Figure 1. Steps performed during V&V secure code reviews by VA Application Development team | 2 |
| Figure 2. V&V secure code review roles and responsibilities..... | 3 |
| Figure 3. V&V secure code review process flow..... | 4 |
| Figure 4. IV&V incident response secure code review roles and responsibilities | 8 |
| Figure 5. IV&V incident response secure code review flow | 9 |

1. Introduction

This document provides a high-level overview of how secure code reviews are conducted agency-wide as part of the VA Information Security (OIS) Software Assurance (SwA) Program. This document provides information to assist VA Application Developers with understanding code review processes, including performing secure code reviews themselves (as opposed to independent secure code reviews performed by the VA SwA Program Office), also known as Verification and Validation (V&V) of their applications both during development and the Assessment and Authorization (A&A) process.

1.1 Document Audience

The processes described in this document are primarily intended for VA Application Developers and stakeholders that support VA SwA Program secure code review processes agency-wide:

VA Application Developers

VA Application Developers may be either VA employees or contractors. The VA application developer performs V&Vs of their own applications during development and supports the VA SwA Program Office with high-risk & high-priority application reviews as needed.

VA SwA Program Office

The VA SwA Program Office maintains and operates an agency-wide software assurance program. Responsibilities include performing validations of developer-performed secure code reviews, providing training, tools, and assistance to VA Application Developers.

VA National Service Desk (NSD)

The VA NSD implements an agency-wide Tier 1 and Tier 2 help desk support function using its ticketing process. Ticketing processes have been created to support the VA SwA Program Office.

VA Certification Program Office (CPO)

The VA CPO implements the A&A process to support Federal Information Security Management Act (FISMA) compliance. The CPO gains its authority, in part, from VA Handbook 6500.3

VA Network Security Operations Center (NSOC)

The VA NSOC provides continuous, around-the-clock monitoring of VA's network. VA NSOC personnel deter, detect, and defeat potential threats that may adversely affect VA networks and systems.

1.2 Secure Code Review Overview

Secure code reviews of VA enterprise applications are conducted during development. Secure code reviews conducted during development are performed both during component testing and during A&A processes. VA Application Developers first open a VA National Service Desk (NSD) ticket to register their application with the VA SwA Program Office.

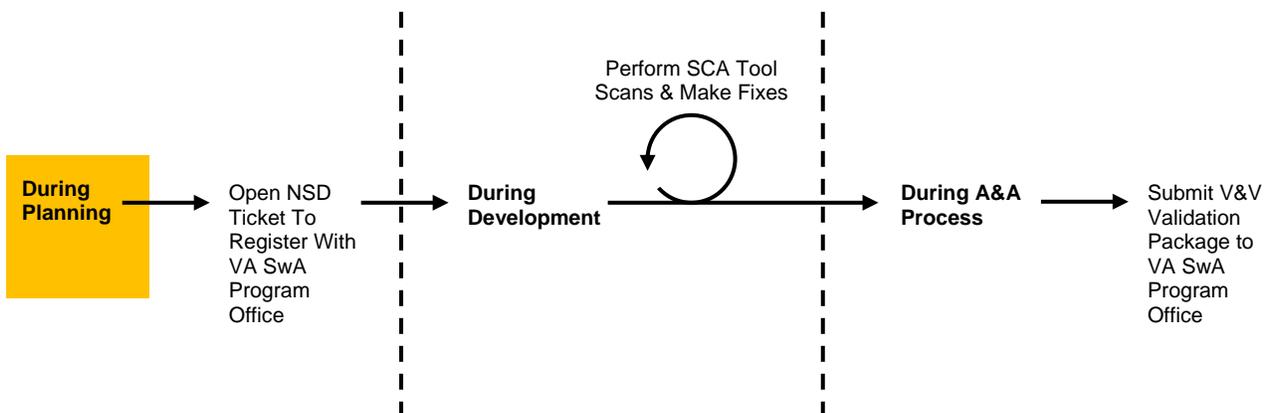
The primary objectives of conducting secure code reviews at the VA are to:

- Encourage the use of static analysis tools during the development of VA applications
- Ensure that secure code reviews are performed consistently and cost-efficiently
- Improve the security of VA applications agency-wide

1.3 V&V Secure Code Reviews

Secure code reviews have been included as activities in the VA ProPath System Development Life Cycle (SDLC) Product Build (BLD) processes since ProPath Release 16.5. System Development processes focus on producing deliverables or artifacts to design, develop, test, implement and support the system as part of an IT project. V&V reviews are included as part of BLD-2 Perform Product Component Test (to conduct secure self-code reviews during development) and as part of BLD-7 Complete Security Controls Assessment (to conduct a milestone code review during the A&A process). Note that BLD-2 and BLD-7 include performing other activities in addition to secure code review. The overall process is depicted in the figure below.

Figure 1. Steps performed during V&V secure code reviews by VA Application Development team



2. V&V Secure Code Reviews

This section describes the process of conducting V&V reviews during the development or maintenance of a VA application by the VA Application Development team. Close cooperation between the OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving secure code review objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities. The goals of performing secure code reviews include making sure that risk-based activities are performed in a secure manner and that V&Vs performed by VA software developers are done correctly and consistently, according to minimum standards prescribed by the VA.

2.1 Roles and Responsibilities

Roles and responsibilities for V&V secure code review processes are described in the figure below.

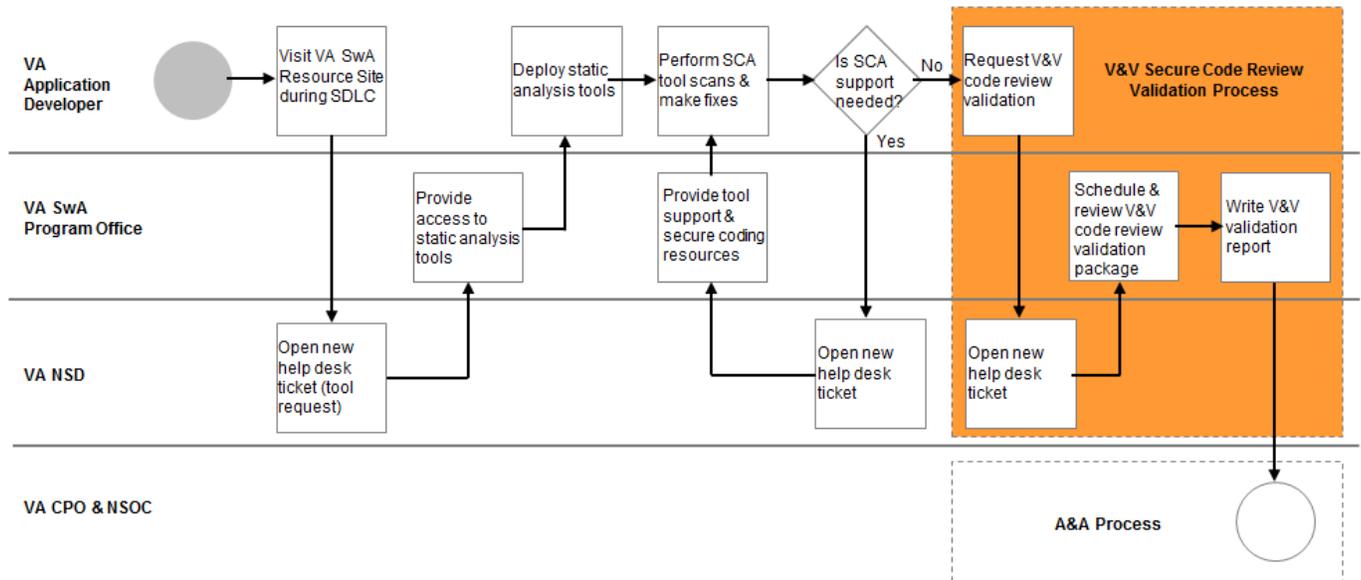
Figure 2. V&V secure code review roles and responsibilities

| VA Application Developer | VA SwA Program Office | VA NSD | VA CPO & NSOC |
|--|---|---|---|
| <ul style="list-style-type: none">• Determine and obtain their program and project needs for secure code reviews, training, tools, and assistance from the VA SwA Program office• Perform V&V secure code reviews during development (as part of component testing)• Perform final V&V secure code reviews during the A&A process• Make fixes to the application source code for which they are responsible (including source code developed by other teams or contractors)• Include mitigations in their application source code for vulnerabilities identified in underlying open source or commercial libraries or frameworks | <ul style="list-style-type: none">• Manage secure code review training (secure coding and application security test tools)• Manage application security test tool licenses• Provide NSD help desk Tier 2 support to provide secure code review assistance to VA Application Developers• Perform validation of secure code reviews conducted by VA Application Developers | <ul style="list-style-type: none">• In support of performing V&V secure code reviews, NSD provides help desk Tier 1 support to VA Application Developers requesting secure code review assistance, and provides the VA SwA Program Office access to the NSD systems for Tier 2 support. | <ul style="list-style-type: none">• Determine whether or not an application is considered high-risk (and thus IV&V is required)• Provide direction to the VA SwA Program Office regarding the prioritization of secure code review validations• Provide A&A requirements and guidelines for obtaining an ATO/TATO |

2.2 Process Overview

A diagram depicting the overall V&V secure code review process flow is depicted below and described in the sections that follow. V&V secure code review validations are intended to be of final application releases during the A&A process as depicted below.

Figure 3. V&V secure code review process flow



2.2.1 Activities During Development

V&V reviews are conducted during development; VA Application Developers scan their own application source code using automated static analysis tools obtained from the VA SwA Program Office. The scan results are used to find and identify potential vulnerabilities and fix early on in the SDLC when it is easiest and most cost-effective to do so. VA Application Developers can leverage training and technical guidance and resources (e.g. automated static analysis tools, secure coding guidelines, etc.) made available by the VA SwA Program Office.

2.2.2 Activities During A&A Process

V&V reviews are conducted during the A&A process to obtain an Authority to Operate (ATO) or Temporary Authority to Operate (TATO). VA Application Developers scan their own application source code and deliver the scan results to the VA SwA Program Office for review. The scan results are reviewed to ensure that best practices for performing secure code review have been followed. The VA SwA Program Office determines whether additional analysis is needed, and assists the VA Application Developers to ensure they understand how to meet the standards required. When the VA SwA Program Office determines that standards have been met, the results are provided to the CPO and NSOC.

2.2.3 Activities During Validation

The VA SwA Program Office performs the following oversight activities during the A&A process:

Review developer-provided scan file review

The static code analysis project file and any custom static analysis tool rulesets are checked that severity thresholds of security vulnerabilities are not exceeded. For example, no “critical” findings should be present in the final scan results.

Review developer-provided custom ruleset review

If custom static analysis tool rulesets were used by the developer to conduct the scan, then these rulesets must be provided for review to determine appropriateness. For example, the rulesets will be checked for any suppression rules that would cause findings to not be reported.

Review developer-provided V&V secure code review request form review

For example, developers must additionally provide documentation on the security controls used by the Application to be reviewed to determine appropriateness. For example, security libraries (e.g. OWASP Enterprise Security API (ESAPI)) should be used, rather than custom developed routines.

2.3 Validation Process

The steps performed by VA Application Developers during the A&A process to request validation of the results of final V&V secure code reviews that they have performed themselves are as follows:

1. Perform a final scan of the application source code
2. Open a NSD ticket to request validation of a final V&V secure code review
3. Provide the VA SwA Program Office with scan results and other requested information
4. Schedule code review validation with the VA SwA Program Office
5. Resolve any issues identified during validation

Details about prerequisites, scheduling, and deliverables are below.

2.3.1 Prerequisites

V&V secure code review validation request packages must contain the following items:

1. V&V secure code review request form that has been filled out (see Appendix A for form download location),
2. Complete and buildable application source code (to use when reviewing scan result file),
3. 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,

4. Static analysis tool scan result file (HP Fortify SCA “.fpr” extension file),
5. 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.
6. 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.
7. The most recent version of Fortify, and the complete, most recent set of the Fortify rulepacks were used when scanning the code.
8. Static analysis tool custom rule file(s) (if any) (HP Fortify SCA “.xml” rulepack file(s))

Note: Applications that are identified as high-risk & high-priority must still also undergo the V&V secure code review process during development and maintenance phases. V&V secure code review validation request packages that are not complete will not be scheduled for validation by the VA SwA Program Office. V&V secure code review validation request packages must be uploaded to the VA SwA Program Office Upload Site provided by the VA SwA Program Office.

2.3.2 Scheduling

After creating a V&V secure code review validation request package, VA Application Developers will need to open a NSD ticket to request validation of a final V&V secure code review. During the validation scheduling process, the VA SwA Program Office will review the provided request package for their completeness (i.e. whether all requested validation request package items have been provided) and then contact the VA Application Developer, CPO, and NSOC as appropriate to schedule validation of package contents (i.e. to perform the VA SwA Program Office technical oversight function). After the review has been scheduled, the V&V secure code review validation schedule that is posted on the VA SwA Program Office Resource Site will be updated.

2.3.3 Deliverables

After a V&V secure code review validation request package has been validated, the following will be provided by the VA SwA Program Office to the VA Application Developer:

1. V&V secure code review validation report (PDF file), and
2. V&V secure code review validation entry on VA SwA Program Office Resource Site (web page)

It is the responsibility of the VA Application Developer to upload the secure code review validation report and final scan results and other deliverables to RiskVision as appropriate.

Appendix A – Resources

VA Office of Information Security Portal – SwA Program Office Resource Site

<https://wiki.mobilehealth.va.gov/display/OISSWA>

VA SwA Program Office Support Requests

The NSD help desk can be contacted at (855) NSD-HELP to request assistance.

OWASP Top Ten

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Enterprise Security API (ESAPI)

https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

CWE/SANS TOP 25 Most Dangerous Software Errors

<https://cwe.mitre.org/top25/>

Appendix B – IV&V Incident Response Secure Code Reviews

This section describes the process of conducting secure code reviews i.e. Independent Verification and Validation (IV&V) for VA applications that have compromised. Based on CPO and NSOC determination an IV&V will be performed by the VA SwA Program Office to ensure the security of an application. These types of reviews are performed by subject matter experts in the areas of application security and secure code review. Secure code reviews are conducted using a semi-automated, tool-assisted methodology developed by the VA Software Assurance Program Office.

Roles and Responsibilities

Roles and responsibilities for IV&V incident response secure code review processes are described in the figure below.

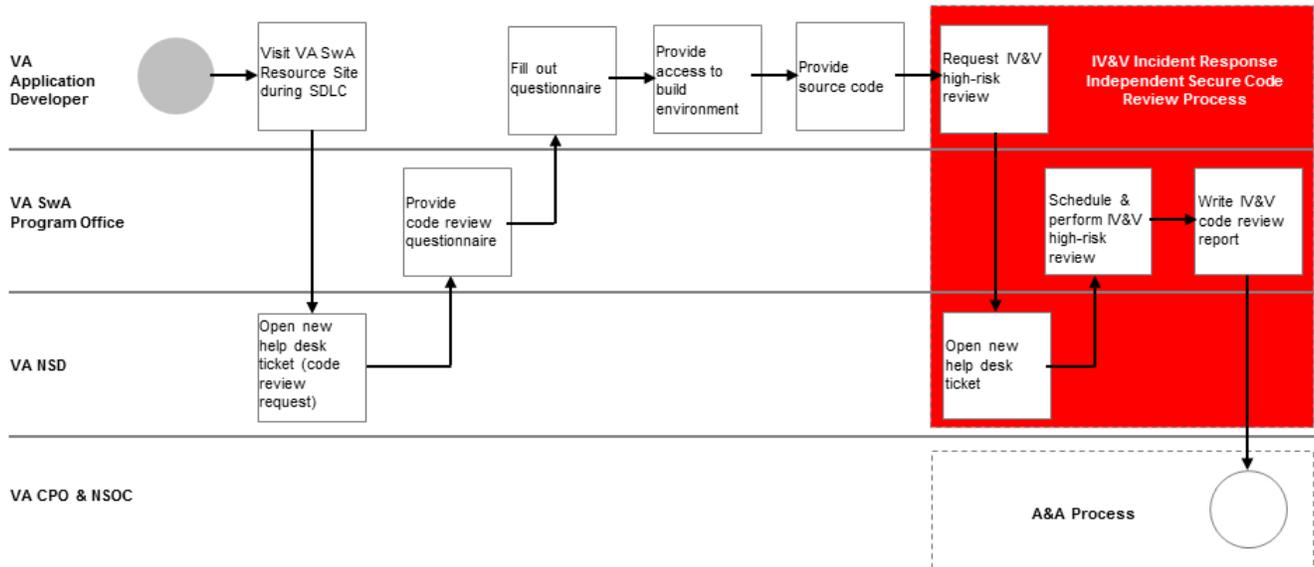
Figure 4. IV&V incident response secure code review roles and responsibilities

| VA Application Developer | VA SwA Program Office | VA NSD | VA CPO & NSOC |
|--|--|---|---|
| <ul style="list-style-type: none">•Support IV&Vs conducted by the VA SwA Program Office•Make fixes to the application source code for which they are responsible (including source code developed by other teams or contractors)•Include mitigations in their application source code for vulnerabilities identified in underlying open source or commercial libraries or frameworks | <ul style="list-style-type: none">•Provide NSD help desk Tier 2 support to provide secure code review assistance to VA Application Developers•Perform secure code reviews of high-risk applications | <ul style="list-style-type: none">•In support of performing IV&V high-risk application reviews, NSD provides help desk Tier 1 support to VA Application Developers requesting secure code review assistance, and provides the VA SwA Program Office access to the NSD systems for Tier 2 support. | <ul style="list-style-type: none">•Determine whether or not an application is considered high-risk•Provide direction to the VA SwA Program Office regarding the prioritization of high-risk secure code reviews•Provide A&A requirements and guidelines for obtaining an ATO/TATO |

Process Overview

A diagram depicting the overall IV&V incident response secure code review process flow is depicted below and described in the sections that follow. IV&V incident response secure code reviews are intended to be of final application releases during the A&A process as depicted below.

Figure 5. IV&V incident response secure code review flow



Incident Response

CPO (in coordination with NSOC) is responsible for initiating incident response activities. Upon this determination, the VA SwA Program Office will conduct an IV&V review of the specified VA application. These types of reviews are performed by subject matter, and may include further analysis of application and respective source code. Further analysis may include examining types of vulnerabilities that can cause concern to the VA, including those that can be found in the current version of the *OWASP Top Ten* and the *CWE/SANS TOP 25 Most Dangerous Software Errors*.

Review Process

The steps performed by VA Application Developers during the A&A process to request IV&V incident response secure code review are as follows:

- Open a NSD ticket to request a IV&V incident response secure code review
- Provide the VA SwA Program Office with source code and other requested information
- Work with the VA SwA Program Office to schedule the review
- Work with the VA SwA Program Office to resolve any issues identified during review

Details about prerequisites, scheduling, and deliverables are below.

Prerequisites

- IV&V incident response secure code review request packages must contain the following items:
- IV&V incident response secure code review questionnaire that has been filled out (see Appendix A for questionnaire download location),
- Complete and buildable application source code (to use to perform the independent secure code review), and
- Access to a remotely-accessible build environment has been provided.

Note: IV&V incident response independent secure code review request packages for initial application reviews must be scheduled 2-3 months in advance. Follow-up independent application reviews may be scheduled as resources and priorities allow. Additional follow-up reviews must be scheduled 2-3 months in advance, or alternately according to a V&V secure code review schedule, depending on CPO or NSOC direction. IV&V incident response secure code review request packages that are not complete will not be scheduled for review by the VA SwA Program Office. IV&V incident response secure code review request packages must be uploaded to the VA SwA Program Office Upload Site provided by the VA SwA Program Office. Access to an upload location on the site must be requested by sending an email to OISSwASupportGroup@va.gov referencing the corresponding NSD ticket number.

Scheduling

After creating an IV&V incident response secure code review request package, VA Application Developers will need to open a NSD ticket to request an IV&V incident response secure code review. During the review scheduling process, the VA SwA Program Office will review the provided request package for their completeness (i.e. whether all requested validation request package items have been provided) and then work with the VA Application Developer, CPO, and NSOC as appropriate to schedule review of package contents (i.e. to perform independent secure code review of the application). After the review has been scheduled, the IV&V incident response secure code review schedule that is posted on the VA SwA Program Office Resource Site will be updated.

Deliverables

After an IV&V incident response secure code review has been performed, the following will be provided by the VA SwA Program Office to the VA Application Developer:

- Long-form IV&V incident response secure code review report (PDF file), and
- Long-form IV&V incident response secure code review report addendum (if manual findings) (Microsoft Word “.docx” extension file),
- Short-form IV&V secure code review report (Microsoft Excel “.xlsx” extension file), and

-
- IV&V incident response secure code review entry on VA SwA Program Office Resource Site (web page)

It is the responsibility of the VA Application Developer to upload the secure code review reports to RiskVision as appropriate.¹

¹ Note that the long-form report is suitable for use as a formal deliverable, whereas the short-form report is intended for use by VA Application Developers as working notes to make it easier to review findings.

