

Secure Code Review Standard Operating Procedures (SOP)

Accreditation Requirements Training

June 2014



Office of Information Security

Objective

The objective of this document is to establish a methodology for conducting secure code reviews throughout the VA enterprise. Developers are to encourage the use of static analysis tools during development, to ensure that secure code reviews are performed consistently and cost-efficiently, and to improve the security of VA applications agency-wide.

Background

The Secure Code Review SOP defines how secure code reviews are conducted agency-wide as part of the VA Information Security (OIS) Software Assurance (SwA) Program.

This document is based on current VA security policies, standards and guidance, and is subject to change as VA and federal policy is modified.

Most current copy of Secure Code Review SOP located:

<https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Secure%20Code%20Review%20SOP.pdf?api=v2>

V&V Secure Code Review 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 minimum VA standards have been met. The VA SwA Program Office determines whether additional analysis is needed, and works with the VA Application Developers to ensure they understand how to meet the standards required.

V&V Secure Code Review Process

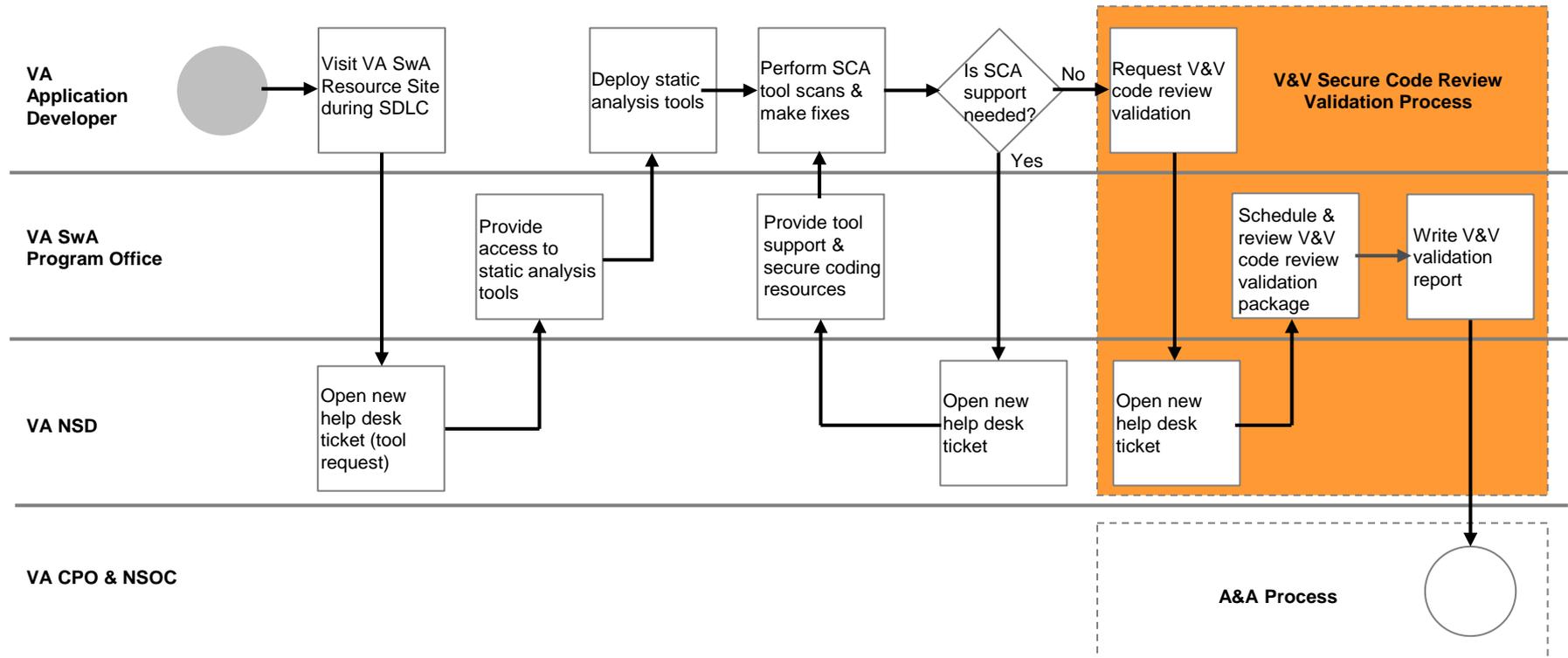
Steps performed by VA Application Developers during the Assessment and Authorization (A&A) process:

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. Work with the VA SwA Program Office to schedule the validation
5. Work with the VA SwA Program Office to resolve any issues identified during validation

VA Application Developers are responsible for performing secure code reviews also known as V&V of their applications both during development and the A&A process.

V&V Secure Code Review Process

V&V secure code reviews integrate with the A&A process as depicted in the figure below.



Closing

Writing secure code is every VA application developer's responsibility. Secure code reviews of VA enterprise applications are conducted at the VA both during development and during the Assessment and Authorization (A&A) process.

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.

The VA Office of Information Security (OIS) Software Assurance (SwA) Program Office maintains and operates the agency-wide software assurance program, including the Secure Code Review SOP.

Resources:

VA SwA Program Office Resource Site:

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

VA SwA Program Office Support Requests:

NSD help desk: (855) NSD-HELP

OWASP Top Ten:

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

CWE/SANS TOP 25 Most Dangerous Software Errors:

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