

CAE-644: FISMA Monitored Securable Custom Module For COTS Application



This page has been made public for vendors

Abstract

The VA custom-developed module for a Commercial Off-the-Shelf (COTS)-based solution has been (or if the module is in development, is intended when in production to be) deployed to a **FISMA-reportable system**, and is scannable using VA-licensed Static Application Security Testing (SAST) tools according to **VA Secure Code Review SOP**.

Note that it is in these cases strongly recommended to register using meaningful names such as:

- E.g. "My Application Name COTS Solution Custom Modules", version 1.0
- E.g. "My Application Portfolio Name COTS Solutions Custom Shared Module", version 1.0

Explanation

All VA applications should ultimately belong to a FISMA-reportable system. The term "monitored" refers to applications that have been deployed to a FISMA-reportable system and as such their operation is being monitored by VA accordingly as components of the system.

VA applications are written in different programming languages, in different development environments, and so on. The term "securable" refers to applications whose source code can be scanned using the VA-licensed HP Fortify Static Code Analyzer (SCA) tool.

Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP, and enforced as part of the ATO issuance process.

References

1. **VA Secure Code Review SOP**
2. "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.
3. "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.
4. HP Fortify System Requirements, current software release.