Government Regulations

Developing software using secure coding rules is a good idea and is increasingly a requirement. The National Defense Authorization Act for Fiscal Year 2013, Section 933, “Improvements in Assurance of Computer Software Procured by the Department of Defense,” requires evidence that government software development and maintenance organizations and contractors conform, in computer software coding, to approved secure coding standards of the Department of Defense (DoD) during software development, upgrade, and maintenance activities, including through the use of inspections and appraisals.


**Application Security and Development STIG, Version 4, Release 8 [DISA 2018]**

Section 2.1 of the Application Security and Development STIG Overview, “Security Assessment Information,” requires that “…coding standards, application vulnerability scan reports, and automated code review results are all part of the suite of system documentation that is expected to be available for review when conducting a security assessment of an application.”

The proper application of this CERT secure coding standard enables a system to comply with the following requirements from the Application Security and Development Security Technical Implementation Guide, Version 4, Release 8:

- (APSC-DV-001995: CAT II) The application must not be vulnerable to race conditions.
- (APSC-DV-002000: CAT II) The application must terminate all network connections associated with a communications session at the end of the session.
- (APSC-DV-002510: CAT I) The application must protect from command injection.
- (APSC-DV-002520: CAT II) The application must protect from canonical representation vulnerabilities.
- (APSC-DV-002530: CAT II) The application must validate all input.
- (APSC-DV-002560: CAT I) The application must not be subject to input handling vulnerabilities.
- (APSC-DV-002590: CAT I) The application must not be vulnerable to overflow attacks.
- (APSC-DV-003215: CAT III) The application development team must follow a set of coding standards.
- (APSC-DV-003235: CAT II) The application must not be subject to error handling vulnerabilities.

Adopting secure coding verification processes and training programmers and software testers on the standard helps to satisfy the following requirements:

- (APSC-DV-003150: CAT II) At least one tester must be designated to test for security flaws in addition to functional testing.
- (APSC-DV-003170: CAT II) An application code review must be performed on the application.
- (APSC-DV-003210: CAT II) Security flaws must be fixed or addressed in the project plan.
- (APSC-DV-003400: CAT II) The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.

**Application Security and Development STIG, Version 3, Release 10 [DISA 2015]**

Section 2.1.5, “Coding Standards,” requires that “the Program Manager will ensure the development team follows a set of coding standards.”

The proper application of this standard enables a system to comply with the following requirements from the Application Security and Development Security Technical Implementation Guide, Version 3, Release 10:

- (APP2060.1: CAT I) The Program Manager will ensure the development team follows a set of coding standards.
- (APP2060.2: CAT II) The Program Manager will ensure the development team creates a list of coding standards to avoid and document this list in the coding standards.
- (APP3550: CAT I) The Designer will ensure the application is not vulnerable to integer arithmetic issues.
- (APP3560: CAT I) The Designer will ensure the application does not contain format string vulnerabilities.
- (APP3570: CAT I) The Designer will ensure the application does not allow command injection.
- (APP3590.1: CAT I) The Designer will ensure the application does not have buffer overflows.
- (APP3590.2: CAT II) The Designer will ensure the application does not use functions known to be vulnerable to buffer overflows.
- (APP3590.3: CAT II) The Designer will ensure the application does not use signed values for memory allocation where permitted by the programming language.
- (APP3600: CAT II) The Designer will ensure the application has no canonical representation vulnerabilities.
- (APP3630.1: CAT II) The Designer will ensure the application is not vulnerable to race conditions.
- (APP3630.2: CAT III) The Designer will ensure the application does not use global variables when local variables could be used.

Training programmers and software testers on the standard helps to satisfy the following requirements:

- (APP2120.3: CAT II) The Program Manager will ensure developers are provided with training on secure design and coding practices on at least an annual basis.
- (APP2120.4: CAT II) The Program Manager will ensure testers are provided training on an annual basis.
- (APP2060.3: CAT II) The Designer will follow the established coding standards established for the project.
- (APP2060.4: CAT II) The Designer will not use unsafe functions documented in the project coding standards.
- (APP5010: CAT III) The Test Manager will ensure at least one tester is designated to test for security flaws in addition to functional testing.