DEPARTMENT OF THE ARMY
OFFICE OF THE PROGRAM EXECUTIVE OFFICER
ENTERPRISE INFORMATION SYSTEMS
(PEO EIS)
9350 HALL ROAD
FORT BELVOIR, VIRGINIA 22060-5526

REPLY TO
ATTENTION OF

SFAE-PS

JUN 0 5 2012

MEMORANDUM FOR PEO EIS Staff Elements, Project/Product Managers (PMs), and Project/Product Directors (PDs)

SUBJECT: PEO EIS Policy Memorandum #12-65, PEO EIS Software Code Reviews (SCR)

1. REFERENCES:

a. DISA Application Security Technical Implementation Guide, 24 July 2008.

b. DoD (8510.10) Information Assurance Certification and Accreditation Process, 28 November 2007.

c. The Directive-Type Memorandum 09-016 "Supply Chain Risk Management (SCRM) to improve the integrity of components used in DoD systems," 25 March 2010.

d. The Program Protection Plan outline and guidance on Software Assurance, July 2010.

e. The FY11 National Defense Authorization Act Section 932 on Software Assurance, 7 January 2011.

1. PURPOSE: This Policy Memorandum provides guidance regarding the implementation of the SCR processes across PEO EIS.

2. DEFINITIONS:

a. SCR is the process by which PEO EIS will analyze all source code by measuring code quality and code assurance across the PEO EIS portfolio.

b. Software Code Quality (SCQ) is an analysis that will evaluate application risk around: robustness (stability), performance, security, transferability and changeability of applications as they evolve. These measurements are based on industry best practices and standards related to complexity, programming practices, architecture, database access and documentation. They are derived from several standard bodies such as the International Standards Organization, Software Engineering Institute, and the National Institute of Standards and Technology among others. PEO EIS will leverage static code analysis tools with quality as its main focus to expose quality defects and ensure that code complies with established code quality metrics.

c. Software Code Assurance (SCA) analyzes software security risk by ensuring that all

Mission software (to include desktop, mobile, cloud, custom, open source, or third party) is trustworthy and in compliance with DoD security mandates. PEO EIS will leverage static code analysis tools with application security as its main focus to expose security vulnerabilities and ensure that code complies with information security practices.

3. APPLICABILITY: This policy applies to all PEO EIS PMs.

4. POLICY:

a. All programs are mandated by PEO EIS to implement the use of Software Code Quality and Software Assurance tools in order to detect errors, enable best practices, find security vulnerabilities, and remediate the applicable vulnerabilities within developed software source code. Commercial off the Shelf software will not be scanned (e.g. MS Office).

b. PEO EIS CIO will centrally provide enterprise licenses for SCQ and SCA to PMs within PEO EIS.

c. PEO EIS will develop a SCR Standard Operating Procedure, which will be followed by all programs.

d. PEO EIS CIO will develop a software scanning schedule and will scan all EIS software assets. At a minimum, these scans will occur annually but may occur on a more frequent basis in conjunction with patches and/or updates.

e. The PEO EIS tools must be utilized before the finalization or release of software into production. PMs are encouraged to use these tools during the development process to improve overall quality and security throughout the software lifecycle.

f. PMs must include the use of SCQ and SCA tools in any and all future contracts involving software development. These contracts must incorporate the use of SCQ and SCA tools within the software development process and/or project schedule.

g. CIO will work with PEO Program Management Division to develop appropriate SCR guidelines and language for inclusion in all future software development contracts.

5. RESPONSIBILITY: My POC for this action is Mr. Michael Herrmann at 703 806-4223, DSN 656-4223, michael.g.herrmann.civ@mail.mil .

DOUGLAS K. WILTSIE
Program Executive Officer