SUBJECT: Secure Coding Governance and Guidance

References: (a) Department of Defense (DoD) Directive 8500.01E,
Information Assurance (IA), 23 April 07
(b) Defense Information Systems Agency (DISA),
Application Security and Development Guide,
24 July 2008
(c) Software Engineering Institute, the CERT C
Secure Coding Standard, 14 October 2008

1. PURPOSE

This Instruction:

1.1 Implements DoD policy, assigns responsibilities, and prescribes procedures for inserting the use of secure coding standards into the development of application software installed onboard surface combatants and submarines.

1.2 Promulgates governance and guidance to integrate secure coding standards into the Acquisition and Systems Engineering processes for systems as an additional element in the overall defense-in-depth architecture.

1.3 Provides Program Managers (PM) and Information Assurance Managers (IAM) with a method to reduce the IA risk from a system compromise due to internal or external malicious attack of custom built software applications.

2. APPLICABILITY

This instruction applies to:

2.1 All Major Defense Acquisition Programs (MDAP - Acquisition Category - ACAT - ID, IC, II, III, IV) and Major Automated Information System Programs (MAISP - ACAT IAM, IAC, III, IV) and other programs that will deliver warfighting capabilities, warfighting mission support systems, or systems deemed critical to military or intelligence missions.

3. DEFINITIONS

Terms used in this instruction are defined in references (a) though (c) or Appendix A

4. POLICY

4.1. This instruction implements DoD IA policies established in reference (a) and the supporting guidance in reference (b).

4.2 Secure Coding Standards Implementation Policy.

In order to comply with the requirement to use coding standards in reference (b), the following policy is established for <to be filled in> systems:

4.2.1 All systems requiring the development of custom software should use a secure coding standard for each selected programming language that incorporates application security principles to promote secure programming practices.

4.2.2 The Software Development Plan should describe how the secure coding standard will be integrated into the development process.

4.2.3 As a neutral Federally Funded Research and Development Center (FFRDC), the Software Engineering Institute (SEI) is the preferred source of coding standards for NAVSEA systems. If custom software is being developed in the C programming language, then the SEI “CERT C Secure Coding Standard” shall be used. In the case of other programming languages where an SEI standard either does not exist or has not been officially released, then the PM will work with the Program IAM and Program Information Assurance System Engineers (IASEs) to develop a secure coding standard based on industry best practices.

4.2.4 Test and evaluation of software should include validation of compliance with the secure coding standard in the Software Test Plan. It is expected that it will be accomplished through the use of static analysis tools and manual reviews.

4.2.5 At least one member of the independent test team should be trained in software security, specifically the vulnerabilities common in the particular programming language(s) used.

5. RESPONSIBILITIES

5.1. The <to be filled in> Command Information Officer (CIO) shall:

5.1.1 Oversee the implementation of this instruction.

5.1.2 Ensure the adjudication of conflicts or disagreements among the <to be filled in> programs and PEOs, and between <to be filled in> Programs and PEOs and other System Command (SYSCOM) Programs and PEOs regarding the procedures and guidelines outlined herein.

5.1.3 Serve as the liaison to the other SYSCOMs for secure coding policy development.

5.2. The <to be filled in> Warfare System Engineer shall:

5.2.1 Ensure the IA effort is adequately staffed and funded to support the IA policies contained herein.

5.2.2 Ensure the <to be filled in> organization supports the integration of secure coding standards into the Acquisition and SE processes.

5.2.3 Ensure the System Engineering Technical Review (SETR) and Naval Warfare System Certification Processes (NSWCP) are aligned to the IA policies contained herein.

5.3. The <to be filled in> Program Executive Officers shall:

5.3.1 Ensure all programs within their purview comply with the DoD IA policies contained herein.

5.3.2 Ensure the Program IASE receives training on software security, with emphasis on training related directly to the vulnerabilities common to the programming languages being used.

5.4. The IA Lead shall:

5.4.4 Serve as the primary Point of Contact within <to be filled in> for coordinating secure coding standards and leveraging lessons learned and existing efforts.

5.4.4 Maintain this document and update it as new secure coding standards are formally released from the SEI.

5.5. The IA Lead shall:

5.5.1. Coordinate with other SYSCOMS IA leads, PEO IAMs, Program IASEs, and Platform Network Engineers to ensure consistent implementation of secure coding standards across programs, PEOs, and SYSCOMs.

6.5.1. Collect and maintain lessons learned from SYSCOMS IA leads, PEO IAMs, Program IASEs, and Platform Network Engineers to ensure continues process improvement.

5.6. The PEO IAM shall:

5.6.1 Coordinate with other PEO IAMs, Program IA System Engineers (IASE), and Platform Network Engineer IA to ensure consistent implementation of secure coding standards across programs, PEOs, and SYSCOMs.

5.6.2 Establish software security training for test and development personnel.

Appendix A
Definitions

A

ACAT	Acquisition Category

C

CERT	Computer Emergency Response Team
CIO	Chief Information Officer

D

DiD	Defense-in-depth
DoD	Department of Defense
DoN	Department of the Navy

F

FFRDC	Federally Funded Research and Development Center

G

G&G	Governance and Guidance

I

IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance System Engineer
IT	Information Technology

M

MDAP	Major Defense Acquisition Programs
MAISP	Major Automated Information System Programs

N

NSWCP	Naval Warfare System Certification Process

P

PEO	Program Executive Office
PM	Program Manager

S

SE	System Engineer
SEI	Software Engineering Institute
SETR Process	System Engineering Technical Review Process
SYSCOM	Systems Command