Implementing Secure Coding Standards in a System Acquisition

John Bergey
Tim Morrow
December 2009
Objective

Explore how required secure coding standards can be appropriately specified and integrated in a system acquisition.

This includes addressing these requirements:

1. Department of Defense (DoD) Directive 8500.01E, Information Assurance (IA), 23 April 07
2. Defense Information Systems Agency (DISA), Application Security and Development Guide,
The Contractual Context and Approach for Integrating Secure Coding Standards

Legend
- PMP – Project Management Plan
- IMS – Integrated master Schedule
- SDP – Software Development Plan
- STP – Software Test Plan
- PDR – Preliminary Design Review
- PCA – Physical Configuration Audit
- FCA – Functional Configuration Audit
- PCA – Physical Configuration Audit
- SRR – System Requirements Review
- DOD IA Directive 8500.01E and DISA AS&D Guide

References
- Secure Coding Standard
- RFP/Contract
- Project Planning
- Language-Specific Secure Coding Standards
- SDP and STP
- Software Development
- Software Testing
- Automated Analysis for Compliance with Secure Coding Standards
- Manual Review of Compliance with Secure Coding Standards
- Secure Coding Analysis Results
- FCA/PCA
- Project Management Process
- SRR
- Action Items

Impact
- Coordination
- Implement
- Document
- Directed toward
- and

Govern
- Requirements
- Mentions
- Requires
- Requires
- Requirements
- Inform
- Input to
- Inform
- Inform
- Action Items
- Action Items

Influence
- Requirements
-Govern
- Produces
-Govern

Security
- Policy
- Deliverable Artifact
- Task or Activity
- Process or Event

Deliverable Artifacts
- Policy
- Task or Activity
- Process or Event

Project Planning
- Secure Coding Standard
- DOD IA Directive 8500.01E and DISA AS&D Guide
- RFP/Contract
- Requirements
- Language-Specific Secure Coding Standards
- SDP and STP
- Software Development
- Software Testing
- Automated Analysis for Compliance with Secure Coding Standards
- Manual Review of Compliance with Secure Coding Standards
- Secure Coding Analysis Results
- FCA/PCA
- Project Management Process
- SRR
- Action Items

Requirements
- Secure Coding Standard
- RFP/Contract
- Requirements
- Language-Specific Secure Coding Standards
- SDP and STP
- Software Development
- Software Testing
- Automated Analysis for Compliance with Secure Coding Standards
- Manual Review of Compliance with Secure Coding Standards
- Secure Coding Analysis Results
- FCA/PCA
- Project Management Process
- SRR
- Action Items