21st Annual NDIA Systems Engineering Conference

Software Assurance Concept of Operations

Advancing Software Assurance in the Modern Age – Part 2

Bradley Lanford, Engility Corporation

In Support for Office of the Under Secretary of Defense for Research and Engineering

October 2018
This CONOPS looks at the fundamental software assurance related processes that program managers should expect to see built in to a system’s development lifecycle.
Top 10 CWEs Mission Dependencies Criticality Analysis

Assurance Knowledge Base

ICD, CDD, CPD, SDD, etc.
Requirements Planning

Decompose

Inform

Document KPPs/TPMs

Inform

SwA Countermeasures

Plan

Inform

SEP

PPP

Engineering SW Assurance Into the Lifecycle

Operational Need
Delivered Capability

Validation Solution

Common Application Across the Acquisition Lifecycle

Design
Product

Assess

Analyze

Metrics Based Reports

Manage SwA Risk

Report

Report

Control Mapping

Prioritize/Mitigate

Report

Report

RMF

Cyber Integrator

Develop

Report

Report

DOPSR Case #18-S-2572
Engineering Software Assurance into the Lifecycle

Operational Need

- Business or Mission Analysis
  - Identify threat environment and opportunities for attack

- Stakeholder Needs & Req Definition
  - Define functional requirements for operation in cyber contested environment

- System Req. Definition
  - Derive non-functional SwA Requirements

- Architecture Definition
  - Develop secure architecture
  - Obtain data rights

- Design Definition
  - Design system with considerations for SwA

- System Analysis
  - Criticality Analysis
  - SwA Evaluation of COTS
  - Submission of TAC Reports
  - Selection of Cybersecurity Controls

Delivered Capability

- Validation Solution

- Requirements

- Integration
  - Full system regression testing
  - Automated reproducible build

- Implementation
  - Warning flags & Coding standards
  - Hardening measures
  - Code reviews

- Verification
  - Static source code weakness analysis
  - Binary Analysis
  - Origin analysis
  - Web app scanners & fuzzers
  - Negative testing
  - Automated test suite w/coverage
  - Penetration Testing

- Operation
  - Implement operational monitoring and response
  - Risk Management Framework (RMF)

- Sustainment and Continuous Engineering
  - Monitor for 3rd party vulnerabilities
  - Continued Assessment & Timely Patching

- Transition
  - Transition data rights
  - Ensure acquirer can rebuild & retest

- Disposal

Continuous Application Across the Acquisition Lifecycle

Design

Product

NOTE: Lifecycle processes typically occur simultaneously, not in sequence; see ISO/IEC 15288 & 12207

NOTE: Implementation, Integration & Verification are often performed continuously & simultaneously with the aid of IDEs & other tools.