Ground Station Architectures Workshop 2001

Improving the Certification and Accreditation Process for DII COE Based Systems

February 21, 2001

Stuart Schaeffer
stuart@aero.org

Charles Lavine
lavine@aero.org

© 2001, The Aerospace Corporation, All Rights Reserved
Topics

• Overview
• Certification & Accreditation
• DII COE
• Common Criteria
• The Problem
• The Solution
Overview

DII COE: Products for Building Systems

DoD Policy

Common Criteria

Security Assurance

Certification & Accreditation (C&A)

DoD Policy

Systems
DoD Regulation 5000.2-R requires that DOD systems be certified and accredited.

- Certification
  - Given security policies and specifications for a particular operating environment, determine the extent to which the system meets the security policy objectives for use in that environment.

- Accreditation
  - Authorization to operate a system under a set of specified conditions.
A “foundation for building systems”: A toolkit of COTS and GOTS software components (OS and middleware), structured in a way to ensure reusability and interoperability in composing a system.

JTA mandates that systems use DII COE components wherever possible.
The Common Criteria

• An international standard (ISO 15408) that provides:
  – A methodology for evaluating how well design and behavior of a product meet the security requirements
  – Catalog of Security Functional and Assurance Requirements
• NSTISSP 11 requires Information Assurance products be evaluated using CC methodology
Common Criteria Methodology

- Product: Component or System
- Security Target
- Certified Evaluation Lab
- Certificate: Conforms to Target
- Evaluation Report
- VPL Validated Product List Entry

Overview
Certification & Accreditation
DII COE
Common Criteria
The Problem
The Solution
The Problem

• C&A requires preparing an evidence package to persuade certifiers that the system meets its security requirements.
  – At present, every program does this in its own way.
• DII COE compliance does not address NSTISSP policy, and does not support C&A
  – Few programs are positioned to meet NSTISSP 11 policy.
The Solution

A process where all programs can capitalize on

- Standard assurance methodology
- Previous analysis and testing
- Existing C&A evidence
The Process Model

Overview
DII COE
Certification & Accreditation
Common Criteria
The Problem
The Solution

S/W Product

Evaluated? (On VPL?)

YES

Get Evaluation Report from VPL

NO

Previous C&A Analysis?

YES

Get from Proposed DII COE Library

NO

Develop Program-Specific Target

Program Performs Security Analysis

Certification Package

Proposed DII COE Library

The Problem

Common Criteria

The Solution

S/W Product

Evaluated? (On VPL?)

YES

Get Evaluation Report from VPL

NO

Previous C&A Analysis?

YES

Get from Proposed DII COE Library

NO

Develop Program-Specific Target

Program Performs Security Analysis

Certification Package

Proposed DII COE Library
CC Evaluations Support C&A

The Problem

Common Criteria

Evaluation Report

Certificate: Conforms to Target

Certification Evidence

Certification Team

Overview
DII COE
Certification & Accreditation
Common Criteria
The Problem ➤ The Solution
Evidence Reuse

- CC Evaluation Evidence
- DII COE Library Evaluation Evidence
- Program-Specific Evaluation Evidence
- Program Selects Needed Documentation
- Certification Package
Overview Revisited

DII COE: Products for Building Systems

DoD Policy

Common Criteria

Security Assurance

DoD Policy

Certification & Accreditation (C&A)

Systems
Improved C&A

Less Effort
Less Time
Lower Costs

Plus

• Standardization
• Uniformity of evidence gathering
• Increased Assurance: evaluated components known to meet their security objectives