



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

Trusted
Computer
Systems
Department



Topics

Overview

Certification &
Accreditation

DII COE

Common
Criteria

The Problem

The Solution

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

Overview



➔ Overview

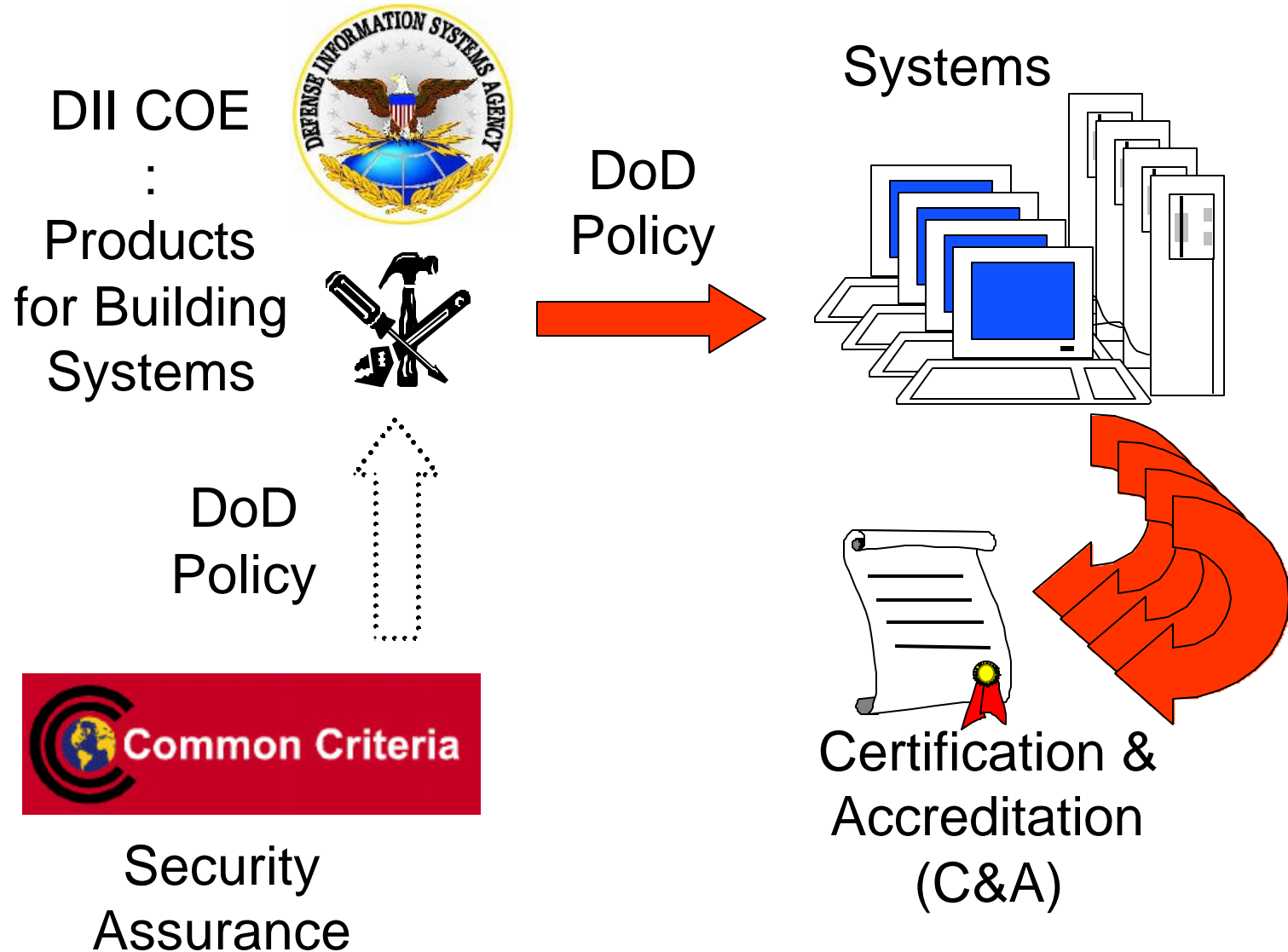
Certification & Accreditation

DII COE

Common Criteria

The Problem

The Solution





Overview

➔ Certification & Accreditation

DII COE

Common Criteria

The Problem

The Solution

Certification and Accreditation



- 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.



DII COE



Overview

Certification &
Accreditation

➔ DII COE

Common
Criteria

The Problem

The Solution

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.



Overview

Certification &
Accreditation

DII COE

➔ Common
Criteria

The Problem

The Solution

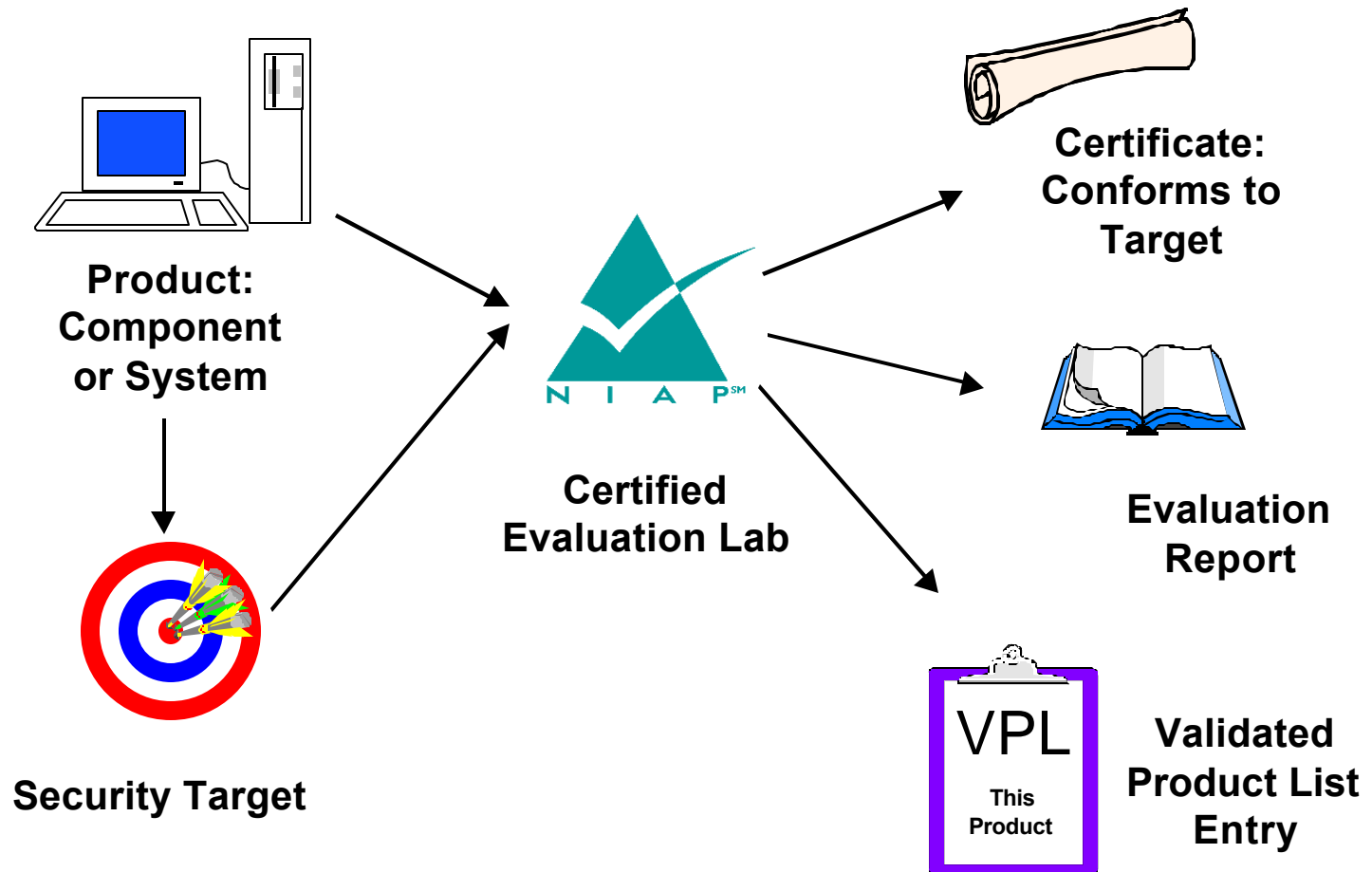
The Common Criteria



- 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

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





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.



Overview

DII COE

Certification &
Accreditation

Common
Criteria

The Problem

➔The Solution

The Solution

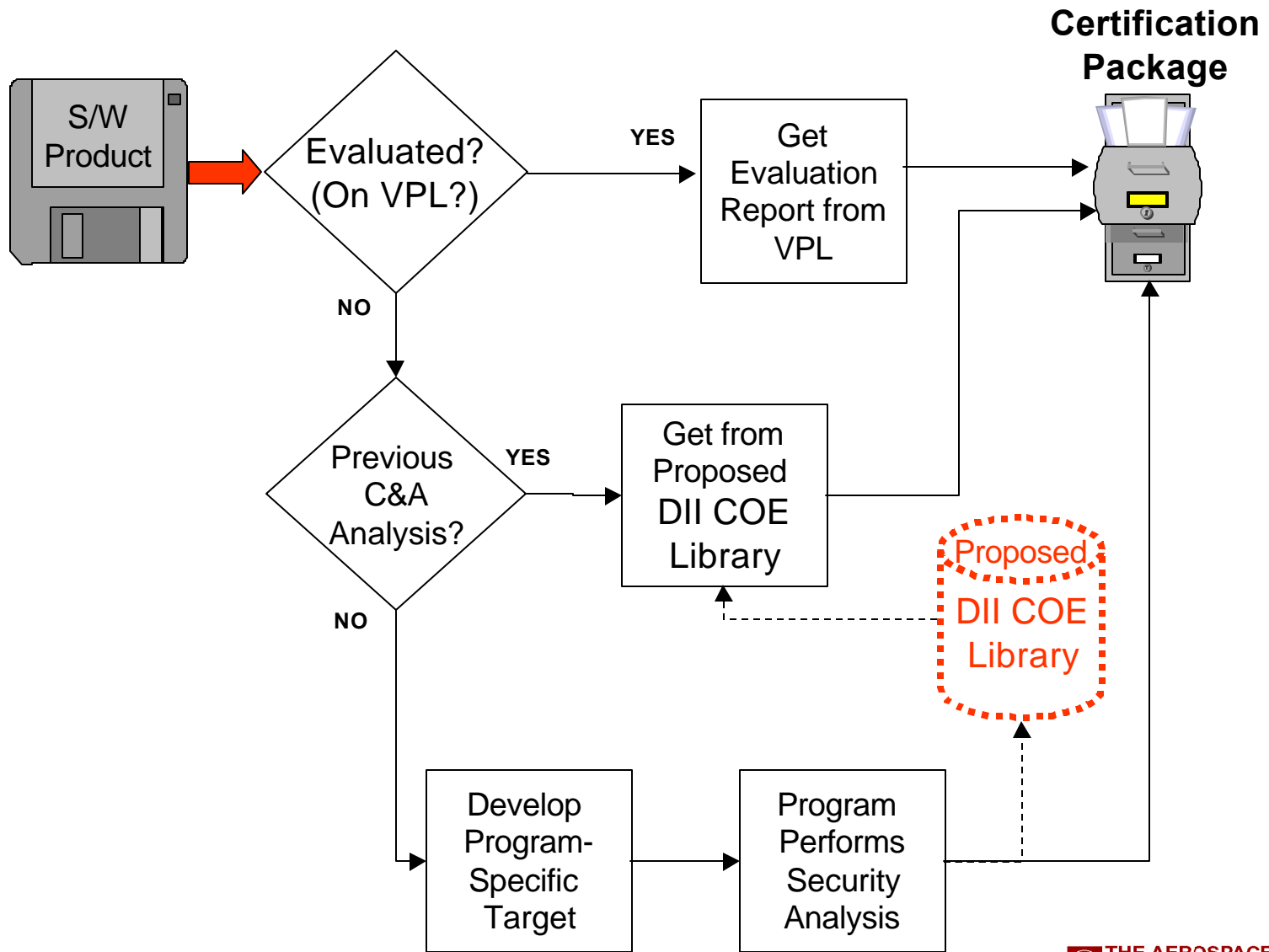
A process where all programs can capitalize on

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



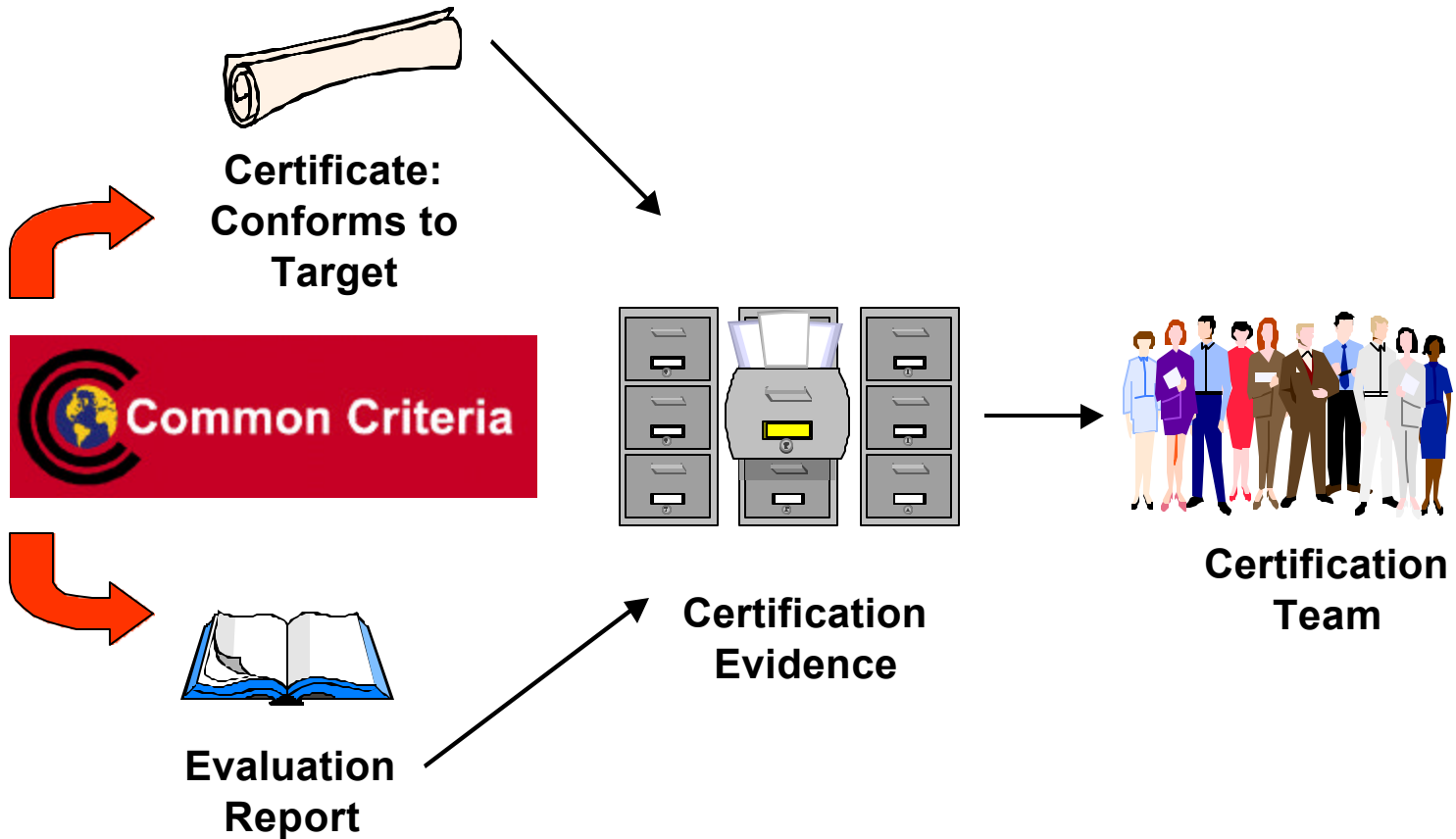
- Overview
- DII COE
- Certification & Accreditation
- Common Criteria
- The Problem
- ➔The Solution

The Process Model



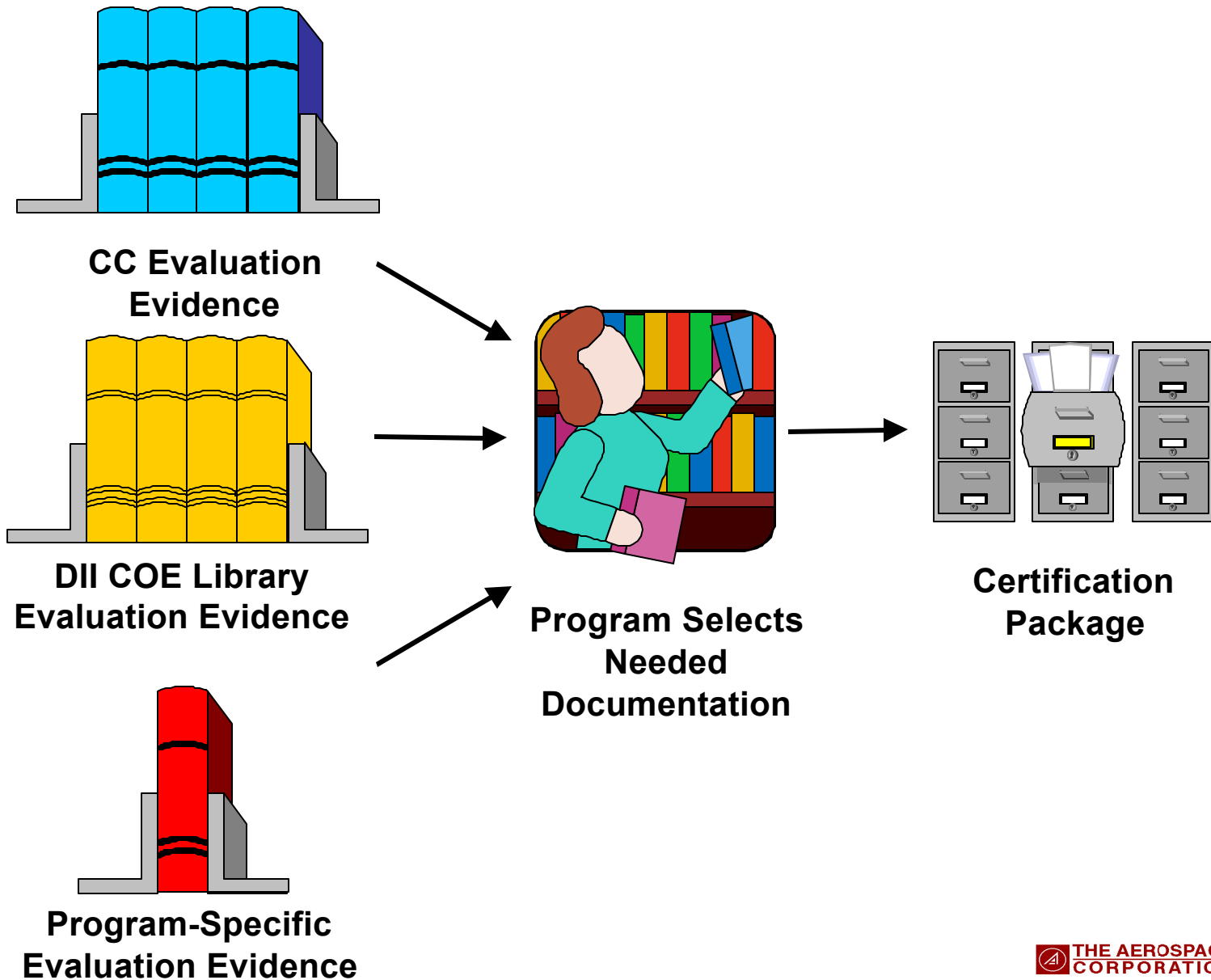
CC Evaluations Support C&A

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



Evidence Reuse

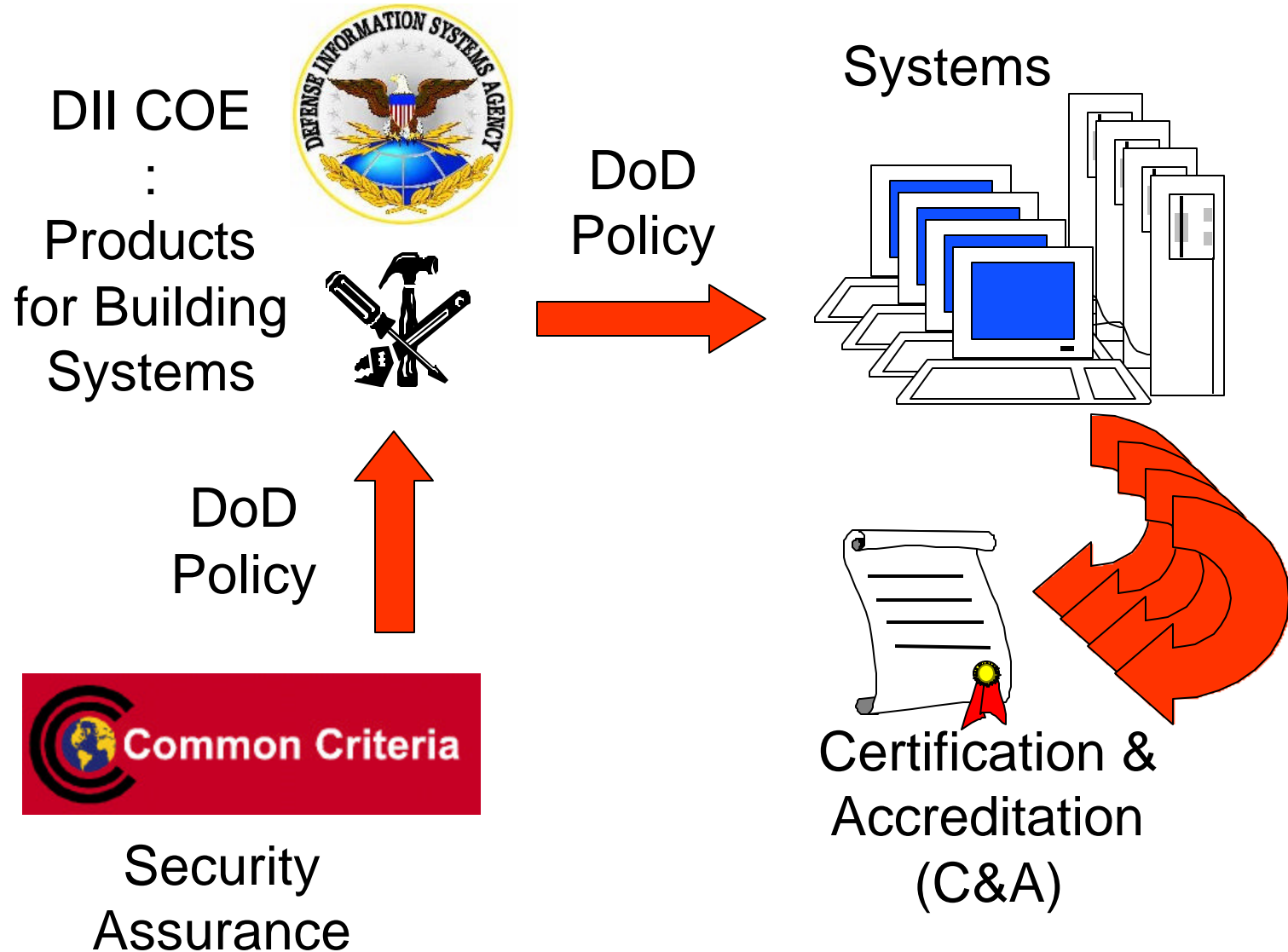
- Overview
- DII COE
- Certification & Accreditation
- Common Criteria
- The Problem
- ➔ The Solution



Overview Revisited



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





Overview

DII COE

Certification &
Accreditation

The Problem

The Common
Criteria

➔The Solution

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