

# Lowering Developer Costs Through Developer Certification

Anthony Hall  
29th September 2005



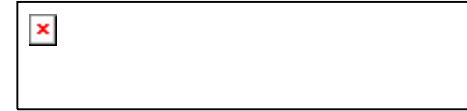
EXPERIENCE. RESULTS.



## Anthony Hall (Senior Evaluator)

- CSC Australia Pty Ltd
- Common Criteria Evaluation Facilities (Australia, North America and Germany)
- AISEF - Australasian Information Security Evaluation Facility
- AISEP - Australasian Information Security Evaluation Program
- E-Mail: [ahall47@csc.com.au](mailto:ahall47@csc.com.au)

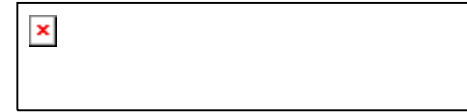




## What will be covered

- Overview
- Current State
- Proposed State
- The Criteria
- Benefits of Change
- Questions

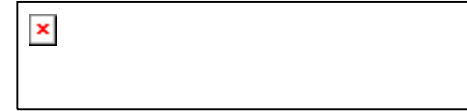




## Overview

- To continue to investigate ways to reduce costs for developer's who are committed to having multiple products evaluated to support the Common Criteria.
- To outline why certifying a site separately will not detract from the assurance provided by the associated components.
- Explore changes that would need to be made in evaluation criteria to show what parts of the criteria would be used, and when these would be used.
- Based of the requirements in Common Criteria Version 2.2.
- Aimed at providing the best financial benefit for the bigger developers that have multiple products evaluated.





## Current State

- Developers are required to provide evidence that security controls on the development environment are adequate to provide Confidentiality and Integrity of the TOE design and implementation. (ALC\_DVS)
- Required for assurance levels of EAL3 – EAL7.
- Needs to be conducted for each new product a developer wishes to have evaluated.
- Increased costs when in many instances evaluating the same site with the same processes and procedures.
- Can be costly if this involves multiple site visits. (Especially if multiple countries are involved)

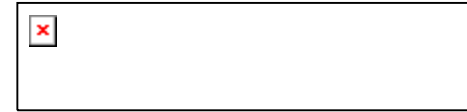




## Proposed State

- Modified process that allows for Developers to have their development environment assessed once. The assessment would cover at least the following:
  - Assess Physical, Personnel and other security measures.
  - Observe the Configuration Management systems in place.
  - Observer the practical delivery measures in place for secure delivery of the TOE.
- Based off the existing Common Criteria requirements.
- Re-assessments required if significant changes have been made to the development environment, significant key staff turnover or on a regular basis. Justification for re-assessments via an Impact Assessment Report.
- For each new product being evaluated Developers could provide an Impact Assessment Report to justify that the development environment “Accredited” was used for development of the TOE.
- Reduced ongoing cost to developers by only having to conduct development environment assessments once.
- Mutual recognition of development environment assessments.





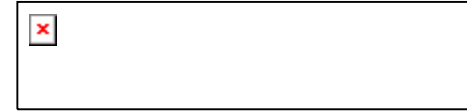
## Proposed State (cont)

- Begin with a modified Security Target to define the scope of the development environment assessment.
- Common Criteria Certified Developer.
- Common Criteria Certified Product.
- Similar to



- Be done as the first part of a normal evaluation process.



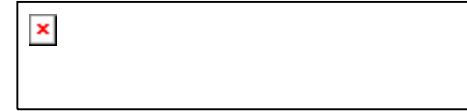


## The Criteria (Example)

- Development Requirements
  - ALC\_DVS
  - ACM\_CAP
  - ADO\_DEL
- TOE Requirements
  - ADV\_FSP
  - ADV\_HLD
  - ADV\_LLD
  - ADV\_IMP
  - ADV\_RCR
  - AGD\_ADM
  - AGD\_USR







## Benefits of Change

- Reduced ongoing evaluation effort by only conducting one initial Developer Certification.
- Reduced effort required by Developers required for multiple development environment assessments.
- Marketing tool to promote that Developers are committed to the Common Criteria evaluation process.
- Common Criteria Certified Developer.
- Common Criteria Certified Product.



Experience. Results.

Questions ?

