Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

SEPTEMBER 2019

Guidelines for Evaluated Products

Evaluated product acquisition

Evaluated products

An evaluated product provides a level of assurance in its security functionality that an unevaluated product does not. To assist in providing this assurance, the Australian Signals Directorate (ASD) performs product evaluations through the following programs:

- ASD Cryptographic Evaluation (ACE) program, for software and ICT equipment that contains cryptographic functionality.
- High Assurance evaluation program, for ICT equipment protecting highly classified information.

The Australian Cyber Security Centre (ACSC) also certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria, as part of the Australasian Information Security Evaluation Program (AISEP).

For organisations seeking to procure evaluated products, the ***Evaluated Products List*** contains a list of products that have been evaluated through the ACE program or the High Assurance evaluation program while the ***Certified Products List*** contains a list of products that have been certified in accordance with the Common Criteria.

Protection Profiles

A Protection Profile (PP) is a technology-specific document that defines the security functions that must be included in a Common Criteria certified product to mitigate specific cyber threats. PPs can be published by a recognised Common Criteria Recognition Arrangement (CCRA) scheme or by the CCRA body itself. PPs published by the CCRA body are referred to as collaborative PPs.

The ACSC recognises all PPs listed on the Common Criteria website in addition to those listed on the ACSC's website. Where a PP does not exist, an evaluation based on an Evaluation Assurance Level (EAL) may be accepted. Such evaluations are capped at EAL2+ as this represents the best balance between completion time and meaningful security assurance gains.

Evaluation documentation

Organisations choosing to use Common Criteria certified products can determine their suitability by reviewing their evaluation documentation. This includes the Security Target and Certification Report.

Products that are undergoing a Common Criteria evaluation will not have published evaluation documentation. However, documentation can be obtained from the ACSC if a product is being evaluated through the AISEP. For a product that is in evaluation through a foreign scheme, the product's vendor can be contacted directly for further information.

Evaluated product selection

A Common Criteria evaluation is traditionally conducted at a specified EAL; however, evaluations against a PP exist outside of this scale. Notably, while products evaluated against a PP will fulfil the Common Criteria EAL requirements, the EAL number will not be published.

Security Control: 0280; Revision: 7; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Should
If procuring an evaluated product, a product that has completed a PP-based evaluation is selected in preference to one that has completed an EAL-based evaluation.

Delivery of evaluated products

It is important that organisations ensure that products they purchase are the actual products that are delivered. In the case of evaluated products, if the product delivered differs from an evaluated version then the assurance gained from the evaluation may not necessarily apply.

Packaging and delivery practices can vary greatly from product to product. For most evaluated products, standard commercial packaging and delivery practices are likely to be sufficient. However, in some cases more secure packaging and delivery practices, including tamper-evident seals and secure transportation, may be required. In the case of the digital delivery of evaluated products, vendor-supplied checksums can often be used to ensure the integrity of software that was delivered.

Security Control: 0285; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Security Control: 0286; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When procuring high assurance ICT equipment, the ACSC is contacted for any equipment-specific delivery procedures.

Further information

Further information on the ACE program is available at https://www.cyber.gov.au/programs/asd-cryptographic-evaluation-program.

Further information on the High Assurance evaluation program is available at https://www.cyber.gov.au/programs/high-assurance-evaluation-program.

Further information on the AISEP is available at https://www.cyber.gov.au/programs/australasian-information-security-evaluation-program.

The ***Evaluated Products List*** is available at https://www.cyber.gov.au/publications/evaluated-products-list.

The ***Certified Products List*** is available at https://commoncriteriaportal.org/products/.

Evaluated product usage

Evaluated configuration

An evaluated product is considered to be operating in an evaluated configuration if:

- functionality that it uses was in the scope of the evaluation and it is implemented in the specified manner

- only product updates that have been assessed through a formal assurance continuity process have been applied
- the environment complies with assumptions or organisational security policies stated in the evaluation documentation.

Unevaluated configuration

An evaluated product is considered to be operating in an unevaluated configuration when it does not meet the requirements of the evaluated configuration and guidance provided in its Certification Report.

Patching evaluated products

In the majority of cases, the latest patched version of an evaluated product will be more secure than an older unpatched version. While the application of patches will not normally place an evaluated product into an unevaluated configuration, some vendors may include new functionality, which has not been evaluated, with their patches. In such cases, organisations should use their judgement to determine whether this deviation from the evaluated configuration constitutes additional security risk or not.

Installation and configuration of evaluated products

Product evaluation provides assurance that a product's security functionality will work as expected when operating in a clearly defined configuration. The scope of the evaluation specifies the security functionality that can be used and how a product is to be configured and operated. Using an evaluated product in an unevaluated configuration could result in the introduction of security vulnerabilities that were not considered as part of the product's evaluation.

For Common Criteria certified products, information is available from vendors regarding its installation, configuration, administration and operation. Additional information is also available in its evaluation documentation. For high assurance ICT equipment, installation and configuration guidance can be obtained from the ACSC.

Security Control: 0289; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Evaluated products are installed, configured, administered and operated in accordance with vendor guidance and evaluation documentation.

Security Control: 0290; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
High assurance ICT equipment is installed, configured, administered and operated in accordance with guidance produced by the ACSC.

Use of high assurance ICT equipment in unevaluated configurations

Given the value of the information being protected by high assurance ICT equipment, it should always be operated in an evaluated configuration.

Security Control: 0292; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
High assurance ICT equipment is only operated in an evaluated configuration.

Further information

Further information on the use of ICT equipment can be found in the ***Guidelines for ICT Equipment Management***.

Further information on patching can be found in the system patching section of the ***Guidelines for System Management***.