Australian Government
Australian Signals Directorate

Information Security Manual

Published: 1 December 2023

Guidelines for Evaluated Products

Evaluated product procurement

High Assurance evaluations

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 evaluations for products used to protect SECRET and TOP SECRET data via its High Assurance Evaluation Program.

Common Criteria evaluations

The Australian Certification Authority within ASD certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria (i.e. the International Organization for Standardization/International Electrotechnical Commission 15408 series), as part of the Australian Information Security Evaluation Program (AISEP).

For an organisation seeking to procure evaluated products, the Common Criteria's *Certified Products List* contains a list of products that have been evaluated, certified and mutually-recognised in accordance with the Common Criteria and the Common Criteria Recognition Arrangement (CCRA).

Cryptographic evaluations

Some CCRA schemes leverage the Cryptographic Algorithm Validation Program for the evaluation of cryptographic algorithms used by cryptographic modules within evaluated products. In such cases, cryptographic evaluations are performed by Cryptographic and Security Testing laboratories that are accredited by the United States' National Voluntary Laboratory Accreditation Program to International Organization for Standardization/International Electrotechnical Commission 17025:2017, *General requirements for the competence of testing and calibration laboratories*.

Protection Profiles

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

ASD recognises all collaborative PPs listed on the Common Criteria website, and will consider national PPs listed on the United States' National Information Assurance Partnership website, in addition to those listed on ASD's AISEP webpage. 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

An organisation choosing to use Common Criteria evaluated 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 ASD 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. In addition, PP modules contain additional requirements that are complementary to or extend upon collaborative PPs. For example, a stateful traffic filtering PP module for a firewall evaluated against a network device collaborative PP. Note, when procuring an evaluated product that has completed a PP-based evaluation, it is important to ensure that all applicable PP modules were included as part of the product's evaluation.

Control: ISM-0280; Revision: 8; Updated: Mar-23; Applicability: All; Essential Eight: N/A
If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules, is selected in preference to one that has completed an EAL-based evaluation.

Delivery of evaluated products

It is important that an organisation ensures that products they source 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, digital signatures or cryptographic checksums can often be used to ensure the integrity of software that was delivered.

Control: ISM-0285; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Control: ISM-0286; Revision: 7; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A
When procuring high assurance ICT equipment, ASD is contacted for any equipment-specific delivery procedures.

Further information

Further information on the High Assurance Evaluation Program is available from ASD.

Further information on the AISEP is available from ASD.

Further information on Common Criteria evaluated products can be found on the Common Criteria's *Certified Products List*.

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

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 maintenance and re-evaluation activities (known as assurance continuity) 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, an organisation should use their judgement to determine whether this deviation from the evaluated configuration constitutes additional security risk or not.

Using 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 installed, configured, administered and operated. Using an evaluated product in an unevaluated configuration could result in the introduction of security risks that were not considered as part of the product's evaluation.

Control: ISM-0289; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A
Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.

Control: ISM-0290; Revision: 8; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A
High assurance ICT equipment is installed, configured, administered and operated in an evaluated configuration and in accordance with ASD guidance.

Further information

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

Further information on the installation, configuration, administration and operation of Common Criteria products is available from vendors and can be found in evaluation documentation on the Common Criteria's *Certified Products List*.

Further information on the installation, configuration, administration and operation of high assurance ICT equipment is available from ASD.