Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 2

EVALUATED PRODUCTS

Version 1.0

Objectives

201. The objective of this handbook is to describe the process of formally evaluating IT security products in Australia. Reference is made to the Common Criteria, the ITSEC, the Australian evaluation process, and the Evaluated Products List.

Evaluation of Security Products

202. The risk management process provides a sound basis from which to mitigate those security threats that could adversely affect the operation of a system. The integrity of those security products or processes employed to mitigate identified risks is usually a critical component of the overall risk management process. In this definition, integrity refers to ensuring the product functions as stated, and more specifically does not contain any "holes" or weaknesses that could render the product ineffective, or worse, provide a false sense of security. There is a multitude of examples where security products, or security functions within other software or hardware products, have been identified as being weak or non-existent. Examples of these "vulnerabilities" include those advisories published by **CERT**, **AusCERT** and **NIPC**.

203. The purpose of the evaluation process is to provide a graded degree of assurance that a product will meet its stated aims in providing security services or functions. This evaluation is undertaken independently of the vendor, to

ensure that the process of evaluation is, in itself, free from bias. Consumers of evaluated products can therefore expect that an evaluated product will have a greater assurance (depending on the assurance level of the product) that it will function as specified by the vendor, based on Internationally agreed standards and accredited facilities.

ITSEC and Common Criteria

204. Up until recently, evaluations in Australia were (and some still are) undertaken in accordance with a European standard called ITSEC. The ITSEC is a harmonised version of some national security evaluation criteria developed by European countries in the early 1990's. These were the United Kingdom, France, The Netherlands and Germany. In short, the ITSEC specifies seven levels of assurance, known as E0 (Inadequate assurance) to E6 (highest assurance). These levels are briefly defined in **Annex A**. A copy of the **ITSEC** is available from the **ITSEC web site.**

205. Although ITSEC gained some leverage from the increased number of nations evaluating security products, it did not include products evaluated by the US or Canada, nor did it provide a framework for mutual recognition of evaluation results between participating countries. The Common Criteria (CC) project was therefore developed to harmonise the evaluation criteria of the European nations, the US and Canada. The aim of the CC was to replace the national criteria with a worldwide standard acceptable to the International Standards Organisation (ISO). The current version of the CC (Version 2.1) was accepted as ISO 15408 on 15 November 1998. Clearly, the benefit of CC is that a vendor can spend resources on evaluating products, with the knowledge and confidence that evaluation results will be accepted by a number of nations, and the product will be listed in the participating nation's registry of evaluated products. CC specifies seven levels of assurance, known as Evaluation Assurance level (EAL) 1 (lowest level) to EAL7 (highest). These levels are briefly defined in **Annex B**. Further information on the CC is available from the US National Institute of Standards and Technology site at **http://www.commoncriteria .org**. A copy of the CC is available from **http://www.isostandards.com.au**.

206. The ITSEC and CC assurance levels are similar, but not identical in their relationship. As a guide, **Table 1** below shows the relationship between the two evaluation criteria. All new evaluations undertaken in Australia will be as per the requirements of the Common Criteria standard, wherever practical.

Common Criteria	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6

Table 1: ITSEC and Common Criteria Evaluation Level Mapping

Mutual Recognition

207. In 1998, Government representatives from United States, Canada, France, Germany and the United Kingdom signed a mutual recognition arrangement for Common Criteria evaluations. Australia and New Zealand signed in October 1999. In May 2000 the group of participating countries expanded to include Norway, Spain,

Netherlands, Italy, Greece and Finland. This group of participating countries is continually expanding. The current list of CCRA participants can be found at **www.commoncriteria.org/registry/NatScheme.html**. The benefits of this mutual recognition are primarily:

a. To ensure that evaluations of IT products are performed to high and consistent standards;

b. To increase the availability of evaluated IT products for national use; and

c. To eliminate duplicate evaluations of IT products.

208. Products procured in a Mutual Recognition environment will therefore not be required to be re-evaluated, but the customer still has an assurance that the standards applied to those products evaluated overseas are the same as those that are applied in Australia. The recognition arrangements therefore cater, amongst other things, for ongoing monitoring of evaluation standards. A Management Committee, composed of senior representatives from each signatory's country, has been established to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities.

209. For Australian Government users it must be noted that whilst DSD will automatically recognise all appropriate certificates issued since the signing of the mutual recognition arrangement, some products evaluated overseas and appearing on DSD's EPL may have caveats attached for their use in Australian Government . In particular, cryptographic products will need to be reviewed by DSD for suitability for use by Australian Government agencies, as per the provisions of **Handbook 9 - Cryptographic Systems**. The point of reference for selecting a product for use in Australian Government is still DSD's EPL.

Australasian Information Security Evaluation Programme

210. Prior to 1995, all information security evaluations were performed by the Defence Signals Directorate (DSD), in its role as the National Computer Security Advisory Authority. To cope with the rising demand for such evaluations, DSD established the Australasian Information Security Evaluation Programme (AISEP).

211. Under the programme, evaluations are performed by impartial companies against the Common Criteria, although some evaluations will still be undertaken under the ITSEC standard. The results of these evaluations are certified by DSD as having rigorously followed the criteria. Only companies licensed by DSD may perform such evaluations. DSD has examined these companies (known as AISEFs - Australasian Information Security Evaluation Facilities) to ensure that they meet the strictest standards of technical expertise, quality control and commercial integrity.

212. The list of currently approved AISEFs can be found at **DSD's website**.

Choosing an Evaluated Product

213. The evaluation of an IT product allows consumers to obtain an impartial assessment of the product by an independent entity. This impartial assessment, or security evaluation, includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. The specific IT product being evaluated is referred to as the Target of Evaluation (TOE). The security requirements for that product are described in its Security Target (ST). An ST details the security features of the product that will enable it to meet its security objectives, the risks that the product may have to protect against and the environment in which the product may have to operate. The ST should be obtained from the developer when determining whether a product meets security needs.

214. To increase the consumer's level of confidence in IT security evaluations, the final evaluation results are reviewed by DSD. This review provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the AISEF are consistent with the facts presented in the evaluation. The impartial evaluation, the independent validation of evaluation results, and the documentation resulting from these processes provide valuable information for consumers about the security capability of IT products.

215. A key to using evaluated products is to ensure that the recommendations of the evaluation are considered in the deployment of the product. These recommendations are contained in a Certification Report, which is available from DSD. Care should be taken to review this information and assess its applicability to the local environment. It is important to note that a TOE will be evaluated under a certain configuration, and may not include features that are normally advertised as part of the product. This may include, but is not limited to, such functions as cryptographic services, graphical user interfaces and configuration tools. There are some general assumptions made about the operational environment where the product is ultimately to be employed subsequent to the security evaluation. The actual environment of use may be significantly different from the one described in the original assumptions in the security target. **Table 2** provides assistance with the minimum levels of assurance that are acceptable for employment of products in a variety of systems with varying classifications. However, it is important to emphasise that these levels are for guidance purposes only, and that DSD advice should be sought to ascertain the evaluation level required for a particular application.

System	IN-CONFIDENCE	PROTECTED	HIGHLY PROTECTED
Public Network/Link Encryption Systems	EAL2 / E1	EAL2 / E1 (Providing the data is decrypted behind an appropriate firewall)	Consult DSD
Remote Access System hard disk encryption	EAL2 / E1	EAL2 / E1 (Providing the data is decrypted behind an appropriate firewall)	Consult DSD

Internet Firewall	EAL2 / E1		EAL4 / E3		EAL6 / E5 (or 2 X EAL4 / E3 systems from different manufacturers with the addition of content filtering, intrusion detection and restricted services)	
Network Separation	**To** PROTECTED	**To** HIGHLY PROTECTED	**To** IN-CONFIDENCE	**To** HIGHLY PROTECTED	**To** IN-CONFIDENCE	**To** PROTECTED
	EAL2 / E1	EAL4 / E3 (however if Internet connection exists EAL6 / E5 required)	EAL2 / E1(however if Internet connection exists EAL4 / E3 required)	EAL4 / E3 (however if Internet connection exists EAL6 / E5 required)	EAL4 / E3(however if Internet connection exists EAL6 / E5 required)	EAL4 / E3(however if Internet connection exists EAL6 / E5 required)
Email Encryption	EAL2 / E1		EAL2 / E1 (Providing the data is decrypted behind an appropriate firewall)		Consult DSD	
Web Encryption	EAL2 / E1		EAL2 / E1 (Providing the data is decrypted behind an appropriate firewall)		Consult DSD	
Gatekeeper CA/RA Software					Consult DSD	

Table 2: Minimum Assurance Level Lookup Table

216. The Evaluated Products List (EPL), which can be viewed at **http://www.dsd.gov.au/infosec/aisep/EPL.html**, indicates which products have completed an evaluation. Products that are currently "in-evaluation" are also on the EPL and can be used subject to acceptance of the risk that the product may not complete evaluation.

AISEP Certificate Extension (ACE) and Assurance Maintenance

217. Evaluation results apply to a specific version of a given product. Any change to that product may invalidate those results. The AISEP Certificate Extension (ACE) program has been devised in order to address the problem posed by the development evolution of certified products. ACE aims to provide a means of maintaining the same level of security assurance without the need for formal re-evaluation until a later time. This is achieved by the developer producing a maintenance plan and appointing a Security Analyst to assess the security impact of all changes affecting the certified product. Potential security problems can be identified and rectified at an early stage with a consequential streamlining of the assurance process. A product which has been accepted into the ACE program will have this noted in its EPL listing.

218. Common criteria also allows for a similar program called Assurance Maintenance. Whilst Assurance Maintenance is not currently recognised under the existing mutual recognition arrangement, products evaluated under the AISEP under CC can still participate in ACE.

219. Australian government agencies wishing to purchase an evaluated product are encouraged to discuss ACE or Assurance Maintenance with the product vendor.

ANNEX A
ITSEC Levels of Assurance Definitions

Each level of assurance detailed below builds upon the previous assurance level.

E0
Inadequate Assurance

E1
A Security Target and description of the architecture must be produced. User /Admin documentation gives guidance on Target of Evaluation (TOE) security. TOE to be uniquely identified and to have Delivery, Configuration, Start-up and Operational documentation. Secure Distribution methods to be utilised. Functional testing is performed by the evaluators, with oversight from DSD.

E2
In addition to the requirements of E1, an informal detailed design, and test documentation must be produced. Architecture also shows the separation of the TOE into security enforcing and other components. Configuration control and developer's security is assessed. Audit trail output is required during start up and operation. Evaluators perform functional and penetration testing with oversight from DSD.

E3
In addition to the requirements of E2, source code or hardware drawings to be produced. Correspondence must be shown between source code and detailed design. Acceptance procedures must be used. Implementation languages should be to recognised standards. Evidence of retesting to be provided after the correction of errors. Evaluators perform functional and penetration testing.

E4
In addition to the requirements of E3, formal model of security and semi-formal specification of security enforcing functions, architecture and detailed design to be produced. Testing must be shown to be sufficient. TOE and tools are under configuration control with changes audited, compiler options documented. TOE to retain security on re-start after failure.

E5
In addition to the requirements of E4, architectural design explains the interrelationship between security enforcing components. Information on integration process and run time libraries to be produced. Configuration control independent of developer. Identification of configured items as security enforcing or security relevant, with support for viable relationships between them.

E6
In addition to the requirements of E5, formal description of architecture and security enforcing functions to be produced. Correspondence shown from formal

specification of security enforcing functions through to source code and tests. Different TOE configurations defined in terms of the formal architectural design. All tools subject to configuration control.

ANNEX B
Common Criteria Levels of Assurance Definitions

The following evaluation levels apply to the Common Criteria (CC) definition.

EAL1
Functionally Tested. Provides analysis of the security functions, using a functional and interface specification of the Target of Evaluation (TOE), to understand the security behaviour. The analysis is supported by independent testing of the security functions, and measured against a Security Target. There is no validation of the cryptography contained within the product at this level.

EAL2
Structurally Tested. Analysis of the security functions using a functional and interface specification and the high-level design of the subsystems of the TOE. Independent testing of the security functions, evidence of developer "black box" testing, and evidence of a development search for obvious vulnerabilities, and measured against a Security Target.

EAL3
Methodically Tested and Checked. The analysis is supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configurations management are also required.

EAL4
Methodically Designed, Tested and Reviewed. Analysis is supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.

EAL5
Semiformally Designed and Tested. Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required.

EAL6
Semiformally Verified Design and Tested. Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be

systematic. Development environment and configuration management controls are further strengthened.

EAL7
Formally Verified Design and Tested. The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.