7

Evaluation of Products under AISEP

Introduction

7.1 The Commonwealth requires the use of products with a high security assurance for the delivery of on-line services and the protection of official information.[1]

7.2 AISEP, the Australasian Information Security Evaluation Program, is the process conducted by the DSD Certification Group to evaluate software products and certify as to their suitability for the security tasks they are claimed to fulfil.[2]

7.3 The program operates on a commercial basis and offers IT security vendors the opportunity to benchmark their products against accepted international standards. Endorsement at the end of the evaluation process provides users, both government and non-government, with an independently assessed level of assurance that the product will meet their individual security needs. [3]

7.4 The Director, DSD has overall responsibility for AISEP, as part of DSD's role as the Commonwealth National Computer Security Advisory Authority. The Director delegates his operational management authority

---

1 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

2 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 2.

3 DSD *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

for AISEP to the Australasian Certification Authority (ACA), that is, the Assistant Secretary, Information Security in DSD.[4]

7.5 AISEP operates under the guidance and advice of a Management Policy Board, chaired by the ACA. The Board provides guidance and advice to the ACA (and indirectly to the Director, DSD) on policy and objectives for the operation of AISEP. It has a broad membership, so as to take account of the requirements of customers, industry and other relevant parties. Its aim is the advancement of evaluation services in both government and industry, while taking account of essential security and commercial interests.[5]

Evaluation Criteria

7.6 When AISEP began in 1994, the evaluation benchmark applied was the Information Technology Security Evaluation Criteria (ITSEC), a standard already used by several countries in Europe. In 1998, an international standard accepted by the International Standards Organisation was incorporated into the system. This standard is based on what are known as the Common Criteria (CC).[6]

7.7 Most of the products currently on the Evaluated Products List were evaluated using ITSEC, which has seven evaluation levels – E0 the lowest, to E6 the highest. New additions are evaluated using the CC. While the CC also has seven levels of assurance, only four levels currently have an established methodology.[7] For the higher levels ITSEC is still used.

7.8 Adoption of an internationally accepted standard has permitted the formation of a Common Criteria Recognition Agreement (CCRA), which Australia and New Zealand joined in 1999. This agreement currently involves 14 countries which accept Certificates from other members of the group, without further assessment. There are two types of participants: seven Certificate Producers[8], who have their own certification / evaluation

4 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 6.

5 DSD, *Exhibit No. 22 Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 6.

6 DSD *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

7 DSD, *Exhibit No. 22 Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 9.

8 Australia, New Zealand, Canada, France, the UK and the USA.

schemes and seven Certificate Consumers[9], who rely on the certificates produced by the Certificate Producer group. The agreement only applies to the first four CC levels. In addition, Australia, New Zealand and the United Kingdom have agreed to recognise their respective ITSEC certificates up to level 6.[10]

Evaluation and Certification Process

7.9 The process of evaluation and certification has three stages[11]:

- *Acceptance*: in which the Target of Evaluation is defined (that is the product or system to be evaluated) and the Security Target is developed (that is the formal statement of the claims made for that product or system). This stage may be undertaken by a licensed evaluation facility – but not by individuals who will be involved in the evaluation process itself.[12] The initial stage ends with DSD assessing the suitability of the Target of Evaluation and the Security Target, plus a preliminary review of any cryptography functions.
- *Evaluation*: The second stage in the process is the evaluation, carried out by a licensed third party known as an Australasian Information Security Evaluation Facility (AISEF).[13] The Certification Group in DSD monitors the work of the AISEF and arranges for the DSD Cryptographic Evaluation section to evaluate any cryptographic security features. When the evaluation is completed, the AISEF issues an Evaluation Technical Report.
- *Certification*: On successful completion of the evaluation, the Certification Group produces a Certification Report; the product is then listed on the Evaluated Products List (EPL) as Evaluated and a Certificate is issued by the ACA.

---

9 Finland, Greece, Italy, Israel, the Netherlands, Norway and Spain.

10 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 4, 23.

11 This section summarised from DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1; DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 9-11.

12 It is a provision of the AISEF licensing agreement that: 'The AISEF shall not:
(b) allow a person who has been involved in the development of the Target of Evaluation to be involved in a Security Evaluation of that Target of Evaluation…' DSD, *Submission 66*, p. 3.

13 To be licensed as an AISEF a facility must be accredited by the Defence Security Branch and the National Association of Testing Authorities, Australia. DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 7-8.

7.10 Products successfully meeting the evaluation criteria are added to the EPL, which is available on the DSD website.[14] This is the definitive list for products evaluated for use in Australian Government systems. It also provides details on products evaluated and certified by other members of the CCRA and which can therefore be accepted for use in Australian Government systems without further evaluation.[15]

7.11 When an evaluation is carried out on a purely commercial basis, DSD charges the company a Certification Fee. That fee is determined from a scale of fees, which increase in line with the level of security assurance required. If the applicant has the written support of a Commonwealth sponsor, however, DSD waives its fee and therefore absorbs the cost.[16]

7.12 The bulk of the fees involved in the evaluation process are paid to the AISEF. The fees charged for pre-evaluation services and evaluations are established on a purely commercial basis between the applicant and its chosen AISEF.[17]

Benefits of AISEP

7.13 The AISEP provides a number of benefits to sponsors, developers and users. Certification under the system:

- gives users a level of assurance that the product will meet a determined level of security needs and comply with internationally recognised criteria;
- allows the product to be used within the Australian and New Zealand governments;
- allows Mutual Recognition by other members of the CCRA;
- gives an opportunity to developers to improve security features in line with customer requests;
- reduces or eliminates the need for further internal security testing;

---

14 DSD Evaluated Product List, http://www.aisep.gov.au/library/epl/epl.html, 28 October 2003.

15 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 5.

16 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 3.

17 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 3.

- enables users to obtain evaluated products from international vendors;
- helps to avoid mistakes which can leave data vulnerable to attack; and
- allows users to cost effectively match products to specified security needs, with an appropriately assured level of performance.[18]

Conflict of Interest

7.14 The commercial advantages to be gained through the certification of a product or process under the AISEP raise the possibility of a conflict of interest arising within an AISEF. Consequently, it is a provision of the AISEF licensing agreement that:

> The AISEF or any employee of the AISEF involved in a Security Evaluation shall not have any commercial, financial, personal or other interest in the outcome of the Security Evaluation.[19]

7.15 Optus expressed some concern that the three companies currently accredited to perform evaluations are also Optus' business competitors:

> We have a situation where we are directly competing against one of them for business and they have all our intellectual property…[20]

7.16 DSD reported that none of the currently licensed evaluation facilities has formally raised a conflict of interest issue. DSD considers that this is mainly due to '… stringent conflict of interest provisions which are contained in the licence agreements under which each of the facilities is required to operate.'[21]

7.17 In addition, each AISEF must operate '… as a separate entity from its parent company, if any, and any other party.'[22]

7.18 DSD gave its opinion that these compulsory contract provisions and the associated power, in the event of a breach, to withdraw an AISEF's status and suspend or terminate the licensing agreement, provides sufficient protection to discourage problems in this area:

---

18 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 3-4.

19 DSD, *Submission No. 66*, p. 3.

20 Ms Reich, *Transcript*, 2 April 2003, p. 202.

21 DSD, *Submission No. 66*, p. 3.

22 DSD, *Submission No. 66*, p. 3.

> Our view is that these conditions provide an adequate degree of separation between the operations of the AISEF and those of the parent company, even in circumstances where the parent company may offer products or services which are potentially in competition with a product that is under evaluation in their facility.[23]

7.19 The Committee has not drawn a conclusion on this issue.

Cost and Duration of the Evaluation Process

7.20 In its submission, Optus claimed that '… getting a product listed on the EPL is expensive and time consuming.' In giving evidence, it added the comment that the process '… acts as a deterrent to list new products.'[24] It also suggested that: 'this system should be less complex, less expensive and faster to complete.'[25]

7.21 Optus indicated that one problem arose from the 'broad-brush' approach of the Protective Security Manual guidelines, used to classify information in the Commonwealth system. This resulted in the highest classification applicable to any information in the system, being applied to *all* the data in the system:

> What tends to happen is that a classification is given which relates to the most valuable information. That then requires a gold-plated solution. Agencies, we think, would get better results and more economic solutions if they imposed multiple security classifications.[26]

7.22 A further comment from Optus, involved the perceived inflexibility of requirements once information has been classified as protected:

> In some instances this had led to the implementation of expensive and unnecessary security solutions.[27]

7.23 Optus' particular complaint is that the security features of the Optus private secure internet have not been recognised – it is treated, Optus said, as being 'untrusted' and no different to the public Internet. Optus noted

---

23 DSD, *Submission No. 66*, p. 4.

24 Mr McCulloch, *Transcript*, 2 April 2003, p. 192.

25 Optus, *Submission No. 30*, p. 6.

26 Mr McCulloch, *Transcript*, 2 April 2003, p. 193.

27 Optus, *Submission No. 50*, p. 2.

that this means that 'an expensive solution – and an unnecessary one, we would submit – needs to be implemented.'[28]

7.24 Indicating the inconsistent security standards applying '… between Commonwealth agencies, between governments and between all levels of government and business', Optus proposed adoption of a graded standard for all organisations handling Commonwealth or personal information.[29]

7.25 As a starting point towards overcoming these shortcomings and inconsistencies, Optus proposed that the process for EPL listing should be streamlined to reduce both the cost and the time taken to complete the requirements. It called attention to a similar recommendation by a Working Group of the MAC. The Working Group proposed:

> Investigating ways and means of improving the process for the Evaluated Products List … which may include a more proactive approach to endorsement to lower the costs and length of time involved in getting products evaluated and on the EPL.[30]

7.26 Optus suggested that classification should take account of the:

- value of the information being protected
- efforts the attacker must undertake to compromise the information; and
- additional costs associated with encrypting 'over classified' information.[31]

7.27 DSD was asked for comments on the evaluation process and its costs. The response noted that the evaluation process is a recognised international standard and that it is rapidly becoming the benchmark for such product evaluations.[32]

7.28 One of the main advantages of the process DSD said, was its international recognition:

> A less extensive process of evaluation would be unlikely to achieve similar international recognition, and would most likely result in vendors having to put their products through a separate evaluation process for every country in which they wished to sell –

---

28 Optus, *Submission No. 50,* p. 2; Mr McCulloch, *Transcript,* 2 April 2003, p. 194.

29 Mr McCulloch, *Transcript*, 2 April 2003, p. 194.

30 Optus, *Submission No. 50,* pp. 1-2; MAC, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* Australian Public Service Commission, 2002, p. 31.

31 Optus, *Submission No. 30,* p. 7; Mr McCulloch, *Transcript,* 2 April 2003, p. 194.

32 DSD, *Submission No. 66,* p. 4.

> the very problem which the Common Criteria was established to address.[33]

7.29 Regarding the costs of the process, DSD explained that its charges are a relatively minor part of the total – and, in fact, are waived when there is a Commonwealth sponsor. Charges for the pre-evaluation and evaluation phases make up the bulk of the cost and are purely commercial charges.[34]

7.30 DSD noted that the total cost of an evaluation is closely linked to the duration of the process. The main factors influencing overall cost are:

- the complexity of the product;
- the scope of the security functionality claimed;
- the level of assurance sought;
- how committed to (and experienced with) the process the vendor is; and
- the extent of the problems identified during the evaluation.[35]

7.31 As an example, DSD said that for a simple product with a low assurance evaluation and no cryptographic functions, the task could be completed in a few months and cost in the tens of thousands of dollars. In contrast, a higher assurance evaluation of a more complex product (such as an operating system) can take years and cost millions of dollars.[36]

7.32 Microsoft Australia was asked for a comparison with the cost of the process in the US. It responded that '… we have not conducted any kind of comparative study or assessment of respective evaluation and EPL processes.' Microsoft added that:

> Because receiving common criteria recognition is such a costly and time and resource-intensive process, we have focused on achieving CC recognition through the US system and are then seeking Mutual Recognition agreements with the national signatories, including Australia.[37]

7.33 The variations inherent in the product types submitted for evaluation make it difficult to compare AISEP with its equivalents overseas. DSD said, however, that vendors in several countries which have their own evaluation schemes have made the commercial decision to have their products evaluated under AISEP, not their own scheme. DSD said that

---

33 DSD, *Submission No. 66*, p. 4.

34 DSD, *Submission No. 66*, p. 4.

35 DSD, *Submission No. 66*, p. 4.

36 DSD, *Submission No. 66*, p. 4.

37 Microsoft Australia, *Submission No. 64*, p. 6.

this indicates that AISEP's performance is regarded as comparable to theirs and cannot be much more expensive.[38]

7.34 Optus said that '… as soon as any changes occur to that hardware or software … you are either living with an older technology … or you are forcing the manufacturer to go through the same process again of spending in the order of half a million dollars to $1 million, plus six to 12 months going through the approval process.'[39]

7.35 The Committee noted, however, that the handbook produced by DSD to explain the AISEP process, indicates in a section on Certificate Maintenance, that upgrades or changes to the product covered by an evaluation will only invalidate the Certificate if the changes affect security aspects.[40] DSD expanded on this concept in its evidence to the Committee:

> … rather than having a product re-evaluated, depending on the scope of the changes, it is possible to go back and assess the security impact of them and issue a certificate extension, which essentially says that the same level of assurance can be maintained about the product.
>
> If the changes are outside that scope or if they specifically add new security functionality requirements, that would mean re-evaluation. But the important thing to remember is that re-evaluation does not mean starting from scratch. If the product is substantially the same, there is reuse of existing material and it might be a relatively painless process.[41]

7.36 The Committee notes that mutual recognition may be a pathway to accreditation for major players like Microsoft, but is a pathway probably not available to smaller companies.

7.37 The booklet encourages the isolation of changes to specific areas of the design or code, so that:

- the changes can be more easily assessed;
- their impact on the Security Target can be more easily assessed; and
- the re-evaluation and re-certification process can be reduced to a minimum.[42]

---

38 DSD, *Submission No. 66,* p. 4.

39 Mr Kidd, *Transcript,* 2 April 2003, p. 195.

40 *Exhibit 22,* p. 17.

41 Mr Scotton, *Transcript,* 16 June 2003, pp. 271-2.

42 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 17.

7.38 As mentioned above, the AISEP Certificate Extension program encourages Sponsors and Developers to adopt a systematic approach to maintaining security assurance for new versions of certified products and systems, without necessarily submitting them to another full evaluation.[43]

Committee Comment

7.39 Initially, the Committee was concerned about claims by witnesses that the expense and time involved in having products accepted for the EPL are acting as a deterrent.[44]

7.40 DSD and NOIE indicated that charges in Australia are not markedly higher than those charged in comparable systems overseas. There was also evidence to indicate that applicants can often substantially reduce the costs and the time required for evaluation and certification, by careful planning and use of the Certificate Maintenance procedures.

7.41 The Committee noted Optus' comments on the need for flexibility in the application of data security measures.[45] It agreed that there should be provision for sensitive or confidential data to be 'quarantined' by the application of a higher level of security. This would be more efficient and cost effective, the Committee said, than applying a high level security classification to a large body of data, most of which would be more appropriately classified at a lower level.

7.42 The Committee strongly supported the comments by Optus and the MAC regarding the need to review and streamline the procedures for certifying products and systems under AISEP. It is important to ensure that security standards are not relaxed; but more efficient processes and procedures should be able to reduce the costs and resources required to ensure that those standards are maintained.[46]

7.43 The Committee believes that assessment should be fair and equally applied to all applicants.

---

43 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 17.

44 Mr McCulloch, *Transcript*, 2 April 2003, p. 192.

45 Mr McCulloch, *Transcript*, 2 April 2003, pp. 193-4.

46 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, pp. 13, 31.