AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2001/19

BAE SYSTEMS

Trusted Filter Version 1.0

Issue 1.0
July 2001

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

The BAE SYSTEMS Trusted Filter is a hardware device that has been designed and developed by BAE SYSTEMS. It is a special purpose device designed to provide RED/BLACK separation in systems where control data which cannot be protected by encryption or other means must cross a RED/BLACK boundary.

This report describes the evaluation findings of the BAE SYSTEMS Trusted Filter Version 1.0 product to the ITSEC Assurance Level E5, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its ITSEC E5 level of assurance. It concludes that the product has met the target Assurance Level of E5.

Originator _____

Matthew Earley
Certifier
Defence Signals Directorate

Approval _____

Katrina Johnson
Assistant Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation _____

Lynwen Connick
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the BAE SYSTEMS Trusted Filter Version 1.0 (hereafter referred to as the Trusted Filter). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner. Other users intending to use this product should seek advice from their relevant security advisory authority to determine its suitability in meeting their particular requirements.

Identification of Target of Evaluation

1.2 The version of the Trusted Filter evaluated was Version 1.0.

1.3 The security functionality offered by the Trusted Filter is implemented in hardware and firmware.

1.4 The Trusted Filter consists of:

a) the trusted filter unit;

b) remote alarm module; and

c) the Trusted Filter Operational Documentation.

1.5 For further details of the evaluated components of the Trusted Filter, including details of how to identify the evaluated version, refer to Appendix C.

Evaluation

1.6 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1,2] respectively).

1.7 The purpose of the evaluation was to provide assurance with respect to the effectiveness of the Target of Evaluation (TOE), the Trusted Filter, in meeting its Security Target (ref [3]). The criteria against which the TOE is judged are expressed in the ITSEC (ref [4]). This describes how the degree of assurance is expressed in terms of the levels E1 to E6 and E0, where the latter indicates that the TOE has failed to meet its targeted level of assurance. The methodology used is described in ITSEM and Evaluation Memoranda 4 and 5 (refs [5,6,7]).

1.8 The evaluation was performed by CMG Admiral between August 1997 and May 2001, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [8]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation.

1.9 The Security Target (ref [3]) claimed an assurance level for the product of E5, and claimed that the hardware mechanisms of the TOE are impregnable to direct attack.

General Points

1.10 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered. However, at the ITSEC E5 level of assurance, this probability is significantly reduced.

1.11 The Trusted Filter product should only be used within the intended environment and in accordance with the method of use as explained in (ref [3]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.12 Ultimately, it is the responsibility of the user to ensure that the Trusted Filter product meets their requirements.

Scope of the Evaluation

1.13 The scope of the evaluation is limited to those claims made in the Security Target. Everything claimed in the Security Target was evaluated by CMG Admiral.

Chapter 2 Security Overview of the Trusted Filter

2.1 Potential users are strongly recommended to read the Security Target (ref [3]). This explains the security functionality of the Trusted Filter product in greater detail, as well as the intended environment and method of use for the product. A summary of the Security Target can be found in Appendix B. A full copy of the Security Target can be obtained from BAE SYSTEMS.

Overview of the TOE

2.2 This section provides a summary of the operational role of the TOE together with the functions it is designed to perform.

2.3 The Trusted Filter is a hardware and firmware product designed by BAE SYSTEMS. It is a special purpose device designed to provide RED/BLACK separation in systems where control data which cannot be protected by encryption or other means must cross a RED/BLACK boundary.

2.4 The Trusted Filter is installed on the RED/BLACK boundary and provides its own RED/BLACK separation. On the RED side, the Trusted Filter connects to communications control equipment which itself is in the RED area. On the BLACK side, the Trusted Filter connects to transmission equipment.

2.5 The Trusted Filter allows the control equipment (on the RED side) to transmit only a specified set of control commands to the transmission equipment (on the BLACK side). The Trusted Filter rejects any sequence of data not recognised as a valid command and raises an alarm to notify the operator. There is one exception to this. If the Trusted Filter has not received at least two valid characters when it rejects a sequence of data, it regards this as garbled data and does not raise the alarm. It will still discard the data and then restart validation with the next character received.

2.6 The Trusted Filter allows transmission equipment to pass data (typically a command response) from the BLACK side to the RED side. The BLACK to RED communication path is constructed to prevent any possible leakage of information back from the RED to BLACK side.

2.7 The Trusted Filter has been designed and constructed to ensure that any single hardware failure will not result in an insecure state.

2.8 A single Trusted Filter unit supports up to four communications channels. Associated with each channel are two diagnostic Light Emitting Diodes (LEDs), one coloured green and labelled "Operate" and the other coloured red and labelled "Alarm".

2.9 The Operate LED indicates the Trusted Filter control program for that channel is executing. The control program includes a "watchdog" feature that requires the control program to periodically reset a hardware timer. Failure to do so will result in the Operate LED being extinguished. This indicates that the Trusted Filter hardware or firmware is faulty.

2.10 The Alarm LED indicates that data which has failed validation has been received on that channel. During normal operation it is possible for the Trusted Filter to receive corrupt data, noise or RED data. If any data is received that fails validation, the data will be discarded and the Alarm LED will be illuminated. It will remain illuminated until the channel is reset or the Trusted Filter is powered off. The channel will continue to process incoming data, restarting validation with the next character received. The Alarm LED is for diagnostic purposes only. The Alarm LED is also illuminated if the control program watchdog fails to reset its hardware timer.

2.11 A push-button labeled "Reset" is provided for each channel and can be used to reset the channel. This invokes a hardware reset of the channel, causing it to go through a start-up sequence.

2.12 The Trusted Filter has an on/off switch to provide mains power to the Trusted Filter's Direct Current (DC) power supply and a single green LED that indicates the presence of DC power. This shows that correct DC voltages are being applied to the communications channels.

2.13 An optional remote alarm panel that combines the status of the four communications channels can also be connected to the Trusted Filter. The remote alarm panel has a single red alarm LED, which illuminates whenever a channel raises an alarm, and a single green safe LED, which is illuminated only if no channel has an alarm raised.

2.14 The remote alarm panel is also equipped with a piezoelectric sounder that activates whenever the remote alarm LED is illuminated. The remote alarm panel would normally be required only where the diagnostic alarm status needs to be indicated at a remote location. The presence or absence of the alarm panel has no impact on the operation of the Trusted Filter.

2.15 The Trusted Filter provides a single security objective to ensure that only valid control data is allowed to pass unencrypted from a RED to a BLACK area, without compromising the confidentiality of the non-control data in the RED area. In doing so, the Trusted Filter implements three Security Enforcing Functions (SEFs).

2.16 More detailed information on the Trusted Filter can be found in the Security Target (ref [3]), and in Appendix B of this report.

Documentation

2.17 Before using the product, administrators should ensure that they are aware of and fully understand the relevant operational documentation. Administrators should ensure that they read Chapter 4 of this document and the Trusted Filter Operational Documentation (ref [9]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of the Trusted Filter followed a course consistent with the generic evaluation work programme described in the ITSEM (ref [5]), with work packages structured around the evaluator actions described in the ITSEC (ref [4]). The results of this work are reported in the ETR (ref [8]) under the ITSEC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [3]).

Assurance Results

Correctness – Construction

3.2 This aspect of the evaluation examined both the development process (including the Security Target, the Architectural and Detailed Designs, and the Implementation) and the development environment where the development took place.

Requirements

3.3 The final version of the Security Target (ref [3]) explained the Security Enforcing Functions (SEFs) and mechanisms provided by the TOE, and contained a product rationale that included the intended method of use, the intended environment and the assumptions about physical, personnel and procedural security. The Security Target also explained how the functionality of the TOE was sufficient to counter the assumed threats.

3.4 The Security Target defined the formal model of security policy enforced by the TOE, and a semiformal specification of the Security Enforcing Functions provided by the TOE. Further, the formal model of security policy provided the informal explanations of how the formal security policy model is satisfied by the Security Target.

3.5 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Security Target and Formal Security Policy Model.

Architectural Design

3.6 The semiformal Architectural Design correctly explained the general structure of the TOE and the external interfaces. The Architectural Design explained how the SEFs from the Security Target are provided and how the architectural structure of the TOE provides for largely independent security enforcing components. The Architectural Design explained that the TOE was structured with two security enforcing components, and how they are

separated from the other [security irrelevant] components.

3.7 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Architectural Design.

Detailed Design

3.8 The final set of Detailed Design documents properly identified all of the security mechanisms, explained the realisation of the SEFs, and provided a mapping of the SEFs and their associated security enforcing mechanisms down to the functional units of the design, and adequately documented the interfaces. The evaluators were able to determine that the design of the security enforcing components excluded all other functionality that was unnecessary for the TOE to enforce security.

3.9 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Detailed Design.

Implementation

3.10 The evaluators were able to determine that the implementation was correct by ensuring that the SEFs identified in the Detailed Design were identifiable and correct in the source code and hardware drawings. The test documentation explained how the developer's tests covered the implementation of the TOE SEFs, and were assessed to be of a standard that allowed for the tests to be repeatable and reproducible.

3.11 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Implementation.

Development Environment

3.12 The evaluators were able to determine that a tool-based configuration control system, appropriate quality practices and procedures, and appropriate levels of physical and procedural security supported the development environment, ensuring the confidentiality and integrity of the TOE and its associated documents during development.

3.13 Apart from one unresolved issue, the evaluators determined that the security of the development environment and the configuration control system did satisfy the ITSEC E5 requirements.

3.14 This issue referred to one of the developer's configuration control tools being unable to audit the time of modification for certain objects under configuration control (even though this tool audits the date and originator details). In response to this issue, the certifiers have determined that since the other configuration control tools support the auditing of time, and that the possibility of relying solely on this tool for the purposes of configuration control is significantly low, that the issue does not impact on the overall

assurance or security of the TOE or its development environment. In addition, it is the developer's intention to resolve this issue as a priority under the AISEP Certificate Extension (ACE) Program before any further Trusted Filter units are manufactured. These reasons have allowed the certifiers to conclude that the configuration control system satisfies the ITSEC E5 requirements and that the reported issue does not affect the overall assurance or security of the TOE or its environment.

3.15 As the TOE contains firmware, the evaluators performed an assessment of programming languages and compilers. The evaluators were able to determine that a well-defined programming language was used in the implementation of the TOE, and that appropriate coding standards and guidelines were applied to the development of the TOE.

3.16 The above results, and the clearance of the outstanding issue by the certifiers, have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Development Environment.

Correctness – Operation

3.17 This aspect of the evaluation examined how the delivery and configuration procedures maintain the security of the TOE, and how operational procedures ensure secure start-up and operation.

3.18 The evaluators determined that the operational documentation (ref [9]) explained the operation of the SEFs relevant to the administrator of the TOE and explained how to operate the TOE in a secure manner.

3.19 The evaluators determined that the startup and operation documentation (ref [9]) explained the procedures for secure startup and operation of the TOE.

3.20 The evaluators determined that the assembly and delivery documentation (refs [9-12]) explained the delivery arrangements from the development environment to the customer site, and that the generation of the TOE for delivery was explained.

3.21 The above results allowed the certifiers to conclude that the TOE met the requirements for ITSEC E5 in regard to its Operational Documentation and Environment.

Effectiveness – Construction

3.22 This aspect of the evaluation dealt with:

(i) the suitability of the TOE's security enforcing functions to counter the threats identified in the Security Target;

(ii) the ability of the security enforcing functions and mechanisms to bind together in a

way that is mutually supportive and provides an integrated and effective whole;

(iii) the ability of the TOE's security mechanisms to withstand direct attack; and

(iv) the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

Suitability Analysis

3.23 The evaluators determined that the developer's Suitability Analysis, with further analysis by the evaluators, demonstrated that all of the threats listed in the Security Target were adequately countered by the stated SEFs and/or by a combination of other physical, personnel or procedural security measures.

3.24 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Suitability Analysis.

Binding Analysis

3.25 The Binding Analysis must analyse all the potential relationships between security enforcing functions and mechanisms to ensure that there is no way for any mechanism or function to conflict with, or contradict the intent of, other security enforcing functions or mechanisms. The evaluators found that the developer's Binding Analysis, with further analysis by the evaluators, demonstrated that it was not possible for any binding element to conflict with or contradict the intent of any other binding element.

3.26 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Binding Analysis.

Strength of Mechanisms Analysis

3.27 The Strength of Mechanisms Analysis correctly identified the mechanisms of the TOE. An analysis was provided that justified the claim that the mechanisms of the TOE were of a type that was impregnable to direct attack.

3.28 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Strength of Mechanisms Analysis.

Construction Vulnerability Assessment

3.29 For this aspect of the evaluation, the evaluators examined the developer's Construction Vulnerability Assessment claiming that no known vulnerabilities in the construction of the TOE could, in practice, compromise security. The evaluators reviewed the developer's Construction Vulnerability Assessment, and also performed their own assessment to find potential vulnerabilities in the TOE, and were unable to find any vulnerabilities in

construction of the TOE not already identified by the developer.

3.30 The developer assessment showed that considerably low-risk covert channels may exist in the final implementation of the command set, but cannot be exploited in the intended environment of the TOE, as it is covered by other, uncompromised, external security measures. Testing by the evaluators determined the covert channel bandwidth to be low in the operational environment, but is largely dependent on the selection of the command set by the appropriate accreditation authority (refer to chapter 4). Further testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities due to its construction.

3.31 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Construction Vulnerability Assessment.

Effectiveness – Operation

3.32 This aspect of the evaluation entailed checking how easy the TOE is to use in a secure manner, and making an assessment of the known vulnerabilities in its operation to determine whether they could, in practice, compromise its security.

Ease of Use Analysis

3.33 The evaluators found that the TOE could not be configured or used in a manner which was insecure but which an Administrator would believe to be secure. Further, the evaluators found that the TOE could be installed and used securely using only the Operational Documentation (ref [9]) as guidance, and that all possible failure modes were adequately documented, along with their effects.

3.34 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Ease of Use.

Operational Vulnerabilities Assessment

3.35 During this part of the evaluation, the evaluators assessed the known vulnerabilities in the operation of the TOE to determine whether they could, in practice, compromise the security of the TOE. The evaluators found that the developer's Operational Vulnerability Assessment correctly identified two vulnerabilities in the operation of the TOE. Analysis and testing of the TOE did not reveal any exploitable vulnerabilities in the operation of the TOE that were not satisfactorily mitigated by other measures.

3.36 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E5 requirements for the Operational Vulnerability Assessment.

Specific Functionality

3.37 The Security Enforcing Functions provided by the Trusted Filter are specified in chapter 3 of the Security Target (ref [3]) and summarised in Appendix B of this report.

3.38 The evaluators found that the product provided the functionality specified in the Security Target (ref [3]).

Discussion of Unresolved Issues

3.39 At the conclusion of the evaluation the evaluators identified one outstanding issue which was addressed during certification. This issue has been identified and discussed in paragraph 3.14. As such, there are no unresolved issues remaining from the evaluation.

General Observations

3.40 The certifiers would like to acknowledge the invaluable assistance provided by BAE SYSTEMS staff during the evaluation. Without the due attention to problems found, and their technical assistance, the process could not have succeeded in the same time frame.

3.41 Further, the certifiers would like to acknowledge the efforts of CMG Admiral in ensuring prompt delivery of the Evaluation Technical Report for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the Evaluation Technical Report (ref [8]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, and the additional evaluation activities performed by the Certification Group, the Australasian Certification Authority has determined that the Trusted Filter has met the requirements of the ITSEC E5 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 1.0 of the product. This certificate is only valid when the Trusted Filter correctly comprises the designated components. These components are identified in Annex C and there is an accompanying description explaining how the administrator can verify this version information on delivery.

Recommendations

4.3 The following recommendations involve information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.

4.4 The Trusted Filter should only be used in accordance with the intended method of use and intended environment, as described in sections 2.3 and 2.4 of the Security Target (ref [3]), including consideration of all physical, personnel and procedural security measures. Further, it is recommended that the Trusted Filter installation be accredited by an appropriate security authority to ensure that the intended environment described in the Security Target (ref [3]), together with the recommendations provided below, exists or has been implemented.

Location of the Trusted Filter

4.5 The Trusted Filter requires connection to transmission equipment in the BLACK area and control equipment in the RED area. **The Trusted Filter does not counter the threat that it could be bypassed by connecting the control equipment directly to the transmission equipment.** It is recommended (as stated in intended method of use) that the Trusted Filter be placed in a physically secure environment to which only authorised personnel have access. In higher security environments, the Trusted Filter should be co-located with the control equipment in a **no-lone zone**.

Tamper Seal and Cable Integrity

4.6 The Trusted Filter is securely mounted in a 19-inch rack. Administrators should ensure that the Trusted Filter is located high in the rack such that the tamper seals are clearly visible. Further, the integrity of the tamper seals should be regularly inspected for any sign of damage or the random dot pattern as explained in the Operational Guidance (ref [9]). A regular inspection procedure should be incorporated into the site or system security plan. **The Administrator should immediately report any discovery of damage or tamper to their appropriate security authority and the command data transfer path should be disabled.**

4.7 When inspecting the tamper seals on the Trusted Filter, administrators should also check the cabling connections from the Trusted Filter to the transmission equipment and the control equipment, to ensure that the Trusted Filter is correctly connected and not bypassed.

Installation Considerations

4.8 The installation of the Trusted Filter is only to be carried out by a qualified BAE SYSTEMS Australia employee shortly after product delivery. Under no circumstances should any other personnel attempt to install, configure or undertake maintenance on the device.

4.9 Each channel of the Trusted Filter is equipped with its own RESET switch, ALARM indicator and OPERATE indicator. Installers and/or administrators should ensure that all indicators are clearly visible so that the operational status of each of the channels can easily be determined. Please note that other than performing periodic security checks on the Trusted Filter, administrators are only required to switch the unit on or off, and to reset any channel that shows an alarm. An administrator will not require any further interaction with the Trusted Filter.

4.10 The evaluated configuration of the Trusted Filter has included a remote alarm module. The remote alarm consists of an ALARM indicator (illuminates if one or more alarms have been raised), a NON-ALARM indicator (illuminates if no alarms have been raised) and an audible sounder (sounds if the ALARM indicator is illuminated). As the Trusted Filter front panel may be obscured due to its location in the rack, administrators should ensure that the placement of the remote alarm module is outside the rack enclosure in a high visibility area.

Operational Considerations for the Trusted Filter

4.11 The intended method of use for the Trusted Filter assumes that the cryptographic equipment used in conjunction with the Trusted Filter is appropriate for the classification of data being transmitted. **Australian Government users are encouraged to contact**

their appropriate security authority to ensure compatible cryptographic equipment is being used with the Trusted Filter.

4.12 While performing periodic security checks of the Trusted Filter, administrators need to be aware that a channel failure will either result in the illumination of the ALARM indicator (possibly flashing intermittently) or the OPERATE indicator to extinguish. In either case, the Trusted Filter unit should be switched off and returned to the BAE SYSTEMS immediately. Furthermore, to prevent bypass, the Trusted Filter will constantly illuminate the ALARM indicator if no commands pass through a channel within a 60-second period. **Note that a Trusted Filter channel is still in operation even if the ALARM indicator is illuminated.**

Guidance for Purchasers - Residual Risk of Covert Channels

4.13 Given that the Trusted Filter protects the confidentiality of information in the RED area from the BLACK area, covert channels are a consideration for prospective purchasers. **The evaluation determined that exploitable 'user assisted' covert channels exist within each of the channels of the Trusted Filter.** These 'user assisted' covert channels require the interaction of a malicious user with the Trusted Filter. Therefore, if the Trusted Filter is only used within its intended operational environment (ref [3]), then these covert channels are unlikely to be exploitable within that operational environment, due to the appropriate security clearance and training of staff. **Australian accreditation authorities should contact DSD for further advice on the residual risk of covert channels, and obtain the classified supplement (ref [13]) to aid the accreditation process.**

Guidance for Purchasers - Approval of the Command Set

4.14 The Trusted Filter has been evaluated and certified with four pre-defined command sets, operating independently on one of the four channels supplied with the Trusted Filter. As indicated in the previous recommendation, the severity of the covert channels is largely dependent on the chosen command set. In particular, the types of parameters and/or arguments supplied to each of the commands will determine the effect of any potential covert channel. Therefore, as differing transmission equipment will require different command sets for interoperability with the Trusted Filter, it is strongly recommended that the command set be approved by an appropriate accreditation authority in order to assess the validity of residual covert channels in their operating environment. **Please note that it is the responsibility of the purchaser to contact their appropriate accreditation authority for approval of the command set.**

4.15 In addition to the above recommendation, the Certification Group recommends that additional command sets be evaluated and certified under the AISEP Certificate Extension (ACE) Program. **Australian Government users should ensure that any command set to be used in Australian Government environments has also been assessed as part of the ACE Program.** This will ensure that any new or modified

command sets are adhering to the evaluated configuration of the original evaluation, thereby maintaining its ITSEC E5 certification status. Please note that such changes (when approved) will be specified in a revised Security Target and indicated on the Evaluated Products List (EPL) entry.

4.16 The following guidance is intended to give an indication on the type of process used by an accreditation authority when determining the appropriateness of a command set. It should only be used as a basic guide and is for information only.

1. The initial candidate set is the set of all valid commands accepted and recognised by the remote transmission equipment.

2. All commands that are not required, or are unlikely to be required in the future, for system operation are removed from the set.

3. All commands that represent an unacceptable security risk are removed from the set. This would include any commands that allow free text, or commands that have a high degree of variability in their parameter lists.

4. The previous step is iterated until, in the opinion of the accreditation authority, the covert channel bandwidth is sufficiently low to be acceptable.

At the end of the process, a sub-set of commands is determined that is sufficient to permit system operation that presents the lowest covert channel bandwidth that is feasible. Once the command sub-set has been defined by the customer and agreed by the accreditation authority, BAE SYSTEMS will be responsible for the design, implementation and testing of the Finite State Transition Tables (FSTTs) which implement and enforce the allowable set of commands (and their parameters) in the Trusted Filter. ACE approval (as discussed above) should also be sought at this time.

Guidance for Purchasers - Delivery Procedures

4.17 Purchasers of the Trusted Filter should note that the delivery procedures must be followed to ensure the authenticity and integrity of the delivered TOE. The Trusted Filter is delivered from the manufacturer's site to the operational site by an appropriately trained and security cleared BAE SYSTEMS Australia employee. It is the responsibility of the deliverer to ensure that the Trusted Filter cannot be interfered with or modified during transit in accordance with specific packaging procedures. **Upon delivery, the BAE SYSTEMS Australia employee should check the integrity of the tamper seals on the supplied unit.** Purchasers may confirm the identity of their Trusted Filter unit by inspecting the rear panel of the unit to reveal the serial number. This serial number should be identical to the one specified on the delivery documentation.

4.18 If a Trusted Filter is not to be installed immediately, purchasers should ensure that the

product is stored in a physically secure environment to which only authorised personnel have access. Further, the integrity of the tamper seals should be regularly inspected for any sign of damage or tamper, as explained in the Operational Guidance (ref [9]). **The purchaser should immediately report any discovery of damage or tamper to their appropriate security authority.**

Appendix A References

Please note that some of the following documents are classified as "EVALUATION-IN-CONFIDENCE" and are not appropriate for public release.

[1] Evaluation Memorandum No. 1 - Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.1, March 1997

[2] Evaluation Memorandum No. 2 - The Licensing of AISEFs
Defence Signals Directorate
EM 2, Issue 1.0, August 1994

[3] Trusted Filter Security Target
BAE SYSTEMS
Issue 1.4, November 2000
(COMMERCIAL-IN-CONFIDENCE)

[4] Information Technology Security Evaluation Criteria (ITSEC)
Commission of the European Communities
CD-71-91-502-EN-C, Version 1.2, June 1991

[5] Information Technology Security Evaluation Methodology (ITSEM)
Commission of the European Communities
Version 1.0, 10 September 1993

[6] Manual of Computer Security Evaluation Part I - Evaluation Procedures
Defence Signals Directorate
EM 4, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[7] Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools
Defence Signals Directorate
EM 5, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[8] Trusted Filter Evaluation Technical Report
CMG Admiral
Issue 1.0, May 2001
(RESTRICTED, EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[9] Trusted Filter Operational Documentation
BAE SYSTEMS
Issue 2.0, July 2000

[10] Software Work Instruction - Work Instruction 14: Trusted Filter Build and Release Procedure
BAE SYSTEMS
Issue 1.0, July 1999
(COMMERCIAL-IN-CONFIDENCE)

[11] Software Work Instruction - Work Instruction 15: Secure Transport of Unclassified Material
BAE SYSTEMS
Issue 1.1, July 2000
(COMMERCIAL-IN-CONFIDENCE)

[12] Installation Work Instruction - Work Instruction 16: Trusted Filter Installation
BAE SYSTEMS
Issue 1.0, November 2000
(COMMERCIAL-IN-CONFIDENCE)

[13] Supplement to the Trusted Filter Certification Report Version 1.0
Defence Signals Directorate
Issue 1.0, June 2001
(COMMERCIAL-IN-CONFIDENCE)

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy.

Product Rationale for the TOE

Security Objectives

B.2 The Trusted Filter has the following IT security objective:

a) **Confidentiality**. The TOE shall ensure only valid control data is allowed to pass unencrypted from a RED to a BLACK area.

Intended Environment and Intended Method of Use

B.3 The Intended Method of Use for the Trusted Filter is:

a) To pass data (e.g. device commands) unencrypted across a RED/BLACK interface. A typical installation of the Trusted Filter is in a communications environment involving remotely controlled transmission equipment. In such an environment, it is assumed commands for controlling the transmission equipment are generated in the RED area but the transmission equipment itself is in a BLACK area. Control commands will be specific to a particular piece of transmission equipment, such as a modem or radio transmitter. Typical commands would be to start or stop data transmission or to change the equipment configuration, such as transmission speeds or frequencies.

B.4 The Intended Environment for the Trusted Filter is:

a) All personnel with access to the Trusted Filter will either be security cleared, or escorted by security cleared personnel.

b) The Trusted Filter enclosure shall be securely mounted in a 19 inch rack at all times, and only removed or replaced by end-user approved personnel.

c) The Trusted Filter enclosure shall only ever be opened by manufacturer approved personnel.

Summary of Security Features of the TOE

B.5 The following Security Enforcing Functions (SEFs) are provided by the Trusted Filter:

Filtering SEF

B.6 The TOE shall ensure, for each channel it controls, that only data strings which are validated against a pre-defined set of allowable control data specific to that channel can be transmitted from a RED to a BLACK area.

Data Diode SEF

B.7 The TOE shall ensure any BLACK to RED data path it controls is strictly one way.

Secure Failure SEF

B.8 The design of the TOE shall ensure that any conceivable failure of any single discrete hardware component shall not compromise the security objective of the TOE.

Appendix C Contents of Distribution Package

Configuration for Evaluation

TOE Version

C.1 The Target of Evaluation is BAE SYSTEMS' Trusted Filter Version 1.0.

Hardware

C.2 There are two hardware components in the Trusted Filter. They are the main Trusted Filter unit and the remote alarm module.

C.3 All hardware elements of the TOE are relied upon to operate correctly in support of the security requirements.

C.4 The hardware elements of the Trusted Filter are as follows:

a) **Trusted Filter unit**: Part Number 640/1/34170/001.

b) **Remote Alarm:** Part Number 640/1/34170/001.

Software

C.5 There are four front-end modules designating each of the four channels of the Trusted Filter, which share a common back end module. They have been individually implemented in firmware and their checksums have been included below.

C.6 All software elements of the TOE are relied upon to operate correctly in support of the security requirements.

C.7 The software versions of the Trusted Filter are as follows:

a) Front End ALE module: Version 1.02, checksum 7ED6.

b) Front End Modem module: Version 1.02, checksum 93A8.

c) Front End ATUC module: Version 1.02, checksum 7F36.

d) Front End Heat Sensor module: Version 1.02, checksum 7F0A.

e) Back End module: Version 1.02, checksum 979A.

Procedures for Determining Version of TOE

C.8 In order that an administrator can determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

C.9 The Trusted Filter is delivered from the manufacturer's site to the operational site by an appropriately trained and security cleared BAE SYSTEMS Australia employee. It is the responsibility of the deliverer to ensure that the Trusted Filter cannot be interfered with or modified during transit in accordance with specific packaging procedures.

C.10 Upon delivery, the BAE SYSTEMS Australia employee should check the integrity of the tamper seals on the supplied unit. Purchasers may confirm the identity of their Trusted Filter unit by inspecting the rear panel of the unit to reveal the serial number. This serial number should be identical to the one specified on the delivery documentation.