AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAMME

Certification Report

Certificate Number: 1999/10

Vision Abell Pty Ltd

Data Diode Device FID003 Version 1.2

Issue 1.0
November 1999

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

The Vision Abell Data Diode Device is a hardware device that provides unidirectional data flow. It is designed to allow for the passage of data from a lower classified (Low side) network to a higher classified (High side) network, while ensuring that information cannot pass through the device in the opposite (High to Low) direction.

This report describes the evaluation findings of the Vision Abell Data Diode Device FID003 Version 1.2 product to the ITSEC Assurance Level E6, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its ITSEC E6 level of assurance. It concludes that the product has met the target Assurance Level of E6.

Originator ____________________

Peter Lilley
Certifier
Defence Signals Directorate

Approval ____________________

Anne Robins
Manager, Australasian Information Security Evaluation Programme
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 Vision Abell Data Diode Device FID003 Version 1.2 (hereafter referred to as the Data Diode Device). 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.

Identification of Target of Evaluation

1.2 The version of the Data Diode Device evaluated was Version 1.2.

1.3 The Data Diode Device is a hardware product. There are no software components associated with the product.

1.4 The Data Diode Device consists of:

a) the data diode;

b) a power supply unit, 90 – 264V AC to 5.1V DC; and

c) the Data Diode Device Administration Manual.

1.5 For further details of the evaluated components of the Data Diode Device, 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 Programme (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 about the effectiveness of the Target of Evaluation (TOE), the Data Diode Device, 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 Admiral Management Services between August 1998 and November 1999, 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 E6, 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 E6 level of assurance, this probability is lowest.

1.11 The Data Diode Device 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 Data Diode Device 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 Admiral Management Services.

Chapter 2 Security Overview of the Data Diode Device

2.1 Potential users are strongly recommended to read the Security Target (ref [3]). This explains the security functionality of the Data Diode Device 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 Vision Abell.

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 Data Diode Device is a hardware only product designed by Vision Abell (VA). It provides unidirectional data flow to allow for the passage of data from a lower classified (Low Side) network to a higher classified (High Side) network, while ensuring that information cannot pass through the device in the opposite (High to Low) direction.

2.4 In its evaluated configuration the Data Diode Device is connected between a low-side network data transmitter and a high-side network data receiver. The security of the unidirectional transfer is implemented in hardware, at the physical layer of the ISO model. Thus, any network protocol that does not require handshaking across the Data Diode Device can be used to provide data transfer (e.g. UDP).

2.5 The Data Diode Device provides a single security objective to allow transfer of information from the low-side network without compromising the confidentiality of information on the high-side network. In doing so, the Data Diode Device implements a single Security Enforcing Function (SEF).

2.6 More detailed information on the Data Diode Device SEF can be found in the Security Target for the Data Diode Device product (ref [3]), and in Appendix B of this report.

Documentation

2.7 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 Interactive Link Data Diode Device Administration Manual (ref [10]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of the Data Diode Device 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 Function (SEF) and mechanism 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 referenced a formal policy and architecture document (ref [9]) that specified the formal model of security policy enforced by the TOE, and a formal specification of the Security Enforcing Function provided by the TOE. Further, the formal model of security policy document 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 E6 in regard to its Security Target and Formal Security Policy Model.

Architectural Design

3.6 The final version of the formal Architectural Design correctly explained the general structure of the TOE and the external interfaces. The Architectural Design explained how the SEF from the Security Target is provided and how the architectural structure of the TOE provides for a largely independent security enforcing component. The Architectural

Design explained that the TOE was structured as a single security enforcing component, and is not separated into security enforcing and other components.

3.7 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 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 SEF, and provided a mapping of the SEF and its associated security enforcing mechanism 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 E6 in regard to its Detailed Design.

Implementation

3.10 The evaluators were able to determine that the implementation was correct by ensuring that the SEF identified in the Detailed Design was identifiable and correct in the hardware drawings, and consistent with the formal specification of the SEF provided in the formal policy and architecture document (ref [9]). The test documentation explained how the developer's tests covered the implementation of the TOE SEF, and were assessed to be of a standard that allowed for the tests to be repeatable and reproducible.

3.11 The evaluators reported an unresolved issue at the conclusion of the evaluation. This issue referred to an inconsistency with the test documentation introduced after changes were made to the developer tests, and was judged by the certifiers not to affect the overall assurance or security of the TOE.

3.12 The above results, and the clearance of these outstanding issue by the certifiers, has enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Implementation.

Development Environment

3.13 The evaluators were able to determine that a tool-based configuration control system, and appropriate levels of physical supported the development environment, personnel and procedural security existed that ensured the confidentiality and integrity of the TOE and its associated documents.

3.14 Apart from two unresolved issues, the evaluators determined that the security of the development environment and the configuration control system did satisfy the ITSEC E6 requirements.

3.15 The first issue referred to a number of objects that were not subject to the configuration control process provided in the developer's configuration management documentation. In response to this issue, the developer migrated these objects into the configuration control system, allowing the certifiers to conclude that the configuration control system satisfied the ITSEC E6 requirements.

3.16 The second issue referred to an error in the developer's security procedures. In response to this issue, the developer initiated a review of the security of the classified development environment and developed an Identification and Authentication (I&A) policy, and an Audit policy for the classified development network. This allowed the certifiers to conduct a further review of the security procedures and conclude that the developer's security environment now satisfied the ITSEC E6 requirements.

3.17 As the TOE consists entirely of hardware, the evaluators performed no assessment of programming languages and compilers.

3.18 The above results, and the clearance of these outstanding issues by the certifiers, has enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Development Environment.

Correctness – Operation

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

3.20 The evaluators determined that the operational documentation (ref [10]) explained the operation of the SEFs relevant to the administrator of the TOE and explained how to operate the TOE in a secure manner.

3.21 The evaluators determined that the startup and operation documentation (ref [10]) explained the procedures for secure startup and operation of the TOE.

3.22 The evaluators determined that the assembly and delivery documentation (ref [11,12]) did not explain the delivery arrangements from the development environment to the customer site, although the generation of the TOE for delivery was explained. Since the delivery procedures were not adequately explained, the procedures were not considered suitable, by the certifiers, to maintain the security of the TOE during operation.

3.23 In response this issue, the developer produced new procedures that were examined by the certifiers. Further recommendations regarding the delivery procedures for the TOE are provided in Chapter 4 and Appendix C.

3.24 The preparation of new delivery procedures allowed the certifiers to conclude that the delivery procedures were adequately explained and appropriate to ensure authenticity of the delivered TOE. Further, the above results allowed the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Operational Documentation and Environment.

Effectiveness – Construction

3.25 This aspect of the evaluation dealt with:

- the suitability of the TOE's security enforcing functions to counter the threats identified in the Security Target;
- 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;
- the ability of the TOE's security mechanisms to withstand direct attack; and
- the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

Suitability Analysis

3.26 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 SEF or by a combination of other physical, personnel or procedural security measures.

3.27 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Suitability Analysis.

Binding Analysis

3.28 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.

3.29 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Binding Analysis.

Strength of Mechanisms Analysis

3.30 The Strength on Mechanisms Analysis correctly identified the mechanism of the TOE. An analysis was provided that justified the claim that the mechanism of the TOE was of a type that was impregnable to direct attack.

3.31 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Strength of Mechanisms Analysis.

Construction Vulnerability Assessment

3.32 For this aspect of the evaluation, the evaluators examined the developer's Construction Vulnerability Assessment that claimed no known vulnerabilities in the construction of the TOE. The evalauators 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. Testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities due to its construction.

3.33 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Construction Vulnerability Assessment.

Effectiveness – Operation

3.34 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

3.35 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 Administration Manual (ref [10]) as guidance, and that all possible failure modes were adequately documented, along with their effects.

3.36 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Ease of Use.

Operational Vulnerabilities Assessment

3.37 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 evaluator's found that the developer's Operational Vulnerability Assessment correctly identified four 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 corrected or countered by other measures.

3.38 The evaluators reported one minor issue that remained unresolved at the conclusion of the evaluation but which was judged by the certifiers not to affect the overall assurance or security of the TOE. The issue referred to an incomplete analysis of the potential impact of operational vulnerabilities. However, the evaluators were able to determine through their own analysis the potential impact of identified operational vulnerabilities in the TOE.

3.39 As a result of the above determinations, the certifiers concluded that the TOE fully met the ITSEC E6 requirements for the Operational Vulnerability Assessment.

Specific Functionality

3.40 The Security Enforcing Function (SEF) provided by the Data Diode Device is specified in section 4.2 of the Security Target (ref [3]) and summarised in Appendix B of this report.

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

Discussion of Unresolved Issues

3.42 At the conclusion of the evaluation, five outstanding issues were identified by the evaluators, which were addressed during certification. These issues have been identified and discussed in previous sections of this chapter. As such, there are no unresolved issues remaining from the evaluation.

General Observations

3.43 The certifiers would like to acknowledge the invaluable assistance provided by Vision Abell 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.

3.44 The certifiers would also like to acknowledge the expert technical assistance of Defence Science and Technology Organisation personnel in assisting with the development of the formal evaluation deliverables.

3.45 Further, the certifiers would like to acknowledge the efforts of Admiral Management Services 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 Data Diode Device has met the requirements of the ITSEC E6 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 1.2 of the product. This certificate is only valid when the Data Diode Device 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 Data Diode Device should only be used in accordance with the intended environment described in section 3.3 of the Security Target (ref [3]), including consideration of all physical, personnel and procedural security measures. Further, it is recommended that the Data Diode Device 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 Data Diode Device and Data Receiver

4.5 The Data Diode Device requires connection to a *data transmitter* on the Low side network and a *data receiver* on the High side network. **The Data Diode Device does not counter the threat that it could be bypassed by connecting the *data transmitter* and the *data receiver*.** It is recommended that the Data Diode Device and the *data receiver* are placed in a physically secure environment to which only authorised personnel have access. In higher security environments, the Data Diode Device may be collocated with the *data receiver* in a **no-lone zone**.

Protocol Considerations

4.6 Administrators should be aware that the protocol required for the transfer of data across the Data Diode Device cannot implement hand-shaking. **Under no circumstances should an Administrator connect a return path from the *data receiver* to the *data transmitter* in order to implement data transfer using a network protocol that uses handshaking (e.g. TCP).** This will invalidate the security objective of the Data Diode Device, and could result in the transmission of information from the High side network to the Low side network.

Tamper Seal and Cable Integrity

4.7 Administrators should locate the Data Diode Device such that the tamper seal is clearly visible. Further, the integrity of the tamper seal should be regularly inspected for any sign of damage or the random dot pattern as explained in the Administration Manual (ref [10]). 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 data transfer path should be disabled.** Administrators should also check the cabling connections from the Data Diode Device to the *data transmitter* and the *data receiver* when checking the integrity of the tamper seal, to ensure that the Data Diode Device is correctly connected.

Integrity and Availability of High Side Network

4.8 **Administrators should note that the Data Diode Device does not counter any threats to the integrity or availability of high side information due to an attack from the low-side network.** It is recommended that transferred data be checked for viruses and other forms of malicious code with an approved tool.

Cabling Requirements

4.9 Administrators should note that only Multimode 62.5/125 micrometre SC-Style cables should be used for connection to the Data Diode Device. **The use of single mode cable may cause the Data Diode Device link indicator to illuminate, without correct function of the device.** This may cause an Administrator to assume an incorrect installation and possibly reverse the connection.

4.10 Administrators should note that the *data transmitter* and *data receiver* both require network interfaces that support Multimode 62.5/125 micrometre SC-Style connections. **It is recommended that the output socket of the *data receiver* and the input socket of the *data transmitter* be plugged, or disabled, to prevent inadvertent connection of the Data Diode Device in the reverse direction.**

Guidance for Purchasers - Delivery Procedures

4.11 Purchasers of the Data Diode Device should note that the delivery procedures must be followed to ensure the authenticity and integrity of the delivered TOE. Purchasers will receive a faxed checklist that confirms serial number and tamper seal details that must be completed and faxed back to the point of dispatch. Receivers of the Data Diode Device should be aware that a warning instruction is provided in the packaging that details actions to be taken upon delivery. A procedure for determining the version of the TOE is provided in Appendix C of this report.

4.12 If a Data Diode Device 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 seal should be regularly inspected for any sign of damage or tamper, as explained in the Administration Manual (ref [10]). **The purchaser should immediately report any discovery of damage or tamper to their appropriate security authority.**

Appendix A References

[1] Evaluation Memorandum No. 1 - Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.0, August 1994

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

[3] Data Diode Device Security Target
Vision Abell Pty Ltd.
Issue 4.0, 5th October 1999
(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] Data Diode Device Evaluation Technical Report
Admiral Management Services
Issue 1.1, November 1999.
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[9] Interactive Link Formal Policy and Architecture
Defence Science and Technology Organisation
Version 3.0, 23rd October 1998.

[10] Data Diode Device Administration Manual
Vision Abell Pty Ltd
Issue 5.0, 15th November 1999
Part Number SUG004-5

[11] Data Diode Device Assembly Procedure
Vision Abell Pty Ltd
96162D01990102, Issue 3.0, 6th October 1999

[12] Infosec Division Work Instruction for Delivery Procedures for Interactive Link Components
Vision Abell Pty Ltd.
Infosec/WI/060201, Issue 1.0, 10th November 1999
(COMMERCIAL-IN-CONFIDENCE)

[13] SECMAN3 (1995) Information Systems Security,
Edition 5, Defence Security Branch

[14] ACSI33 Australian Communications Electronic Security Instruction: Security Guidelines for Australian Government IT Systems
April 1998
Defence Signals Directorate

[15] ASSRO Supplement 1 Part A: Australian SIGINT Security Regulations and Orders - Security Standards for SI Systems.
October 1998
Defence Signals Directorate
(RESTRICTED)

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 Data Diode Device has the following IT security objective:

a) **Confidentiality**. The information on the High Side Network is kept confidential from the Low Side Network.

Intended Environment and Intended Method of Use

B.3 The Intended Method of Use for the Data Diode Device is:

a) To pass data *pushed* from the Low Side network to the High Side network. The security of the transfer is implemented in hardware, at the physical layer of the ISO reference model. Any network protocol could be used to implement the transfer if no handshaking across the Data Diode Device is required. UDP is an example of an acceptable protocol that could be used to implement unidirectional data flow of information.

B.4 The Intended Environment for the Data Diode Device is:

a) The Data Diode Device shall be operated in an environment that meets the requirements of SECMAN3 (ref[13]), ACSI33 (ref[14]) or ASSRO Supplement 1 (ref[15]).

b) The Data Diode Device shall be operated and stored in accordance with the requirements of the network with the highest classification. Since this device requires no administrator control after it has been installed, it is the system manager/administrator's responsibility to protect the Data Diode Device from accidental or deliberate tampering which may result in its functionality being bypassed.

c) The Data Diode Device shall be operated in an environment where physical (or some other) security measures prevent any TEMPEST attack.

d) The Data Diode Device case shall be sealed with SCEC (Securities Construction and Equipment Committee) endorsed tamper evident seals that indicate if access to the device has been attempted. The tamper evident seal shall be located in a clearly visible location and the system manager/administrator shall be responsible for monitoring the Data Diode Device tamper seal.

e) System management staff using the Administration Manual shall install the Data Diode Device. The installation of the Data Diode Device is required to be accredited by the appropriate security authority.

f) The Data Diode Device operating environment shall include virus scanners or appropriate mechanisms on the High and Low Side Networks to maintain integrity and availability to the desired level of assurance. Integrity and Availability aspects are not part of the Data Diode Device security objective. Integrity and Availability need to be considered when addressing the total security of the combination of both the High and Low Side Networks when connecting by a Data Diode Device.

g) All staff who have access to classified information shall be trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the information system security is maintained.

Summary of Security Features of the TOE

B.5 The following Security Enforcing Function (SEF) is provided by the Data Diode Device:

Data Diode Device SEF

B.6 **SF1**

Data Diode Function: To prevent data from being transmitted from the High Side Network to the Low Side Network, while allowing data to be transmitted from the Low Side Network to the High Side Network.

This function ensures that data flows from the Low Side Network to the High Side Network and that processes, application or Users on the Low Side Network cannot get access to the information on the High Side Network via the Data Diode Device in accordance with the security objective.

The data can be passed from the Low Side Network, to the High Side Network via the Data Diode Device and the data on the High Side Network is kept confidential from the Low Side Network. The Data Diode Device is implemented in hardware and guarantees that data cannot flow from the High Side Network to the Low Side Network. There is no “back channel”, for communication handshaking, which could be used as a covert channel. It shall be implemented using a purpose built fibre transmitter and receiver, constructed from discrete components. This approach has been adopted to minimise the emanation and the TEMPEST security threat.

Appendix C Contents of Distribution Package

Configuration for Evaluation

Hardware

C.1 The hardware component of the TOE subject to evaluation was the Data Diode Device FID003 Version 1.2.

C.2 All hardware elements of the TOE are relied upon to operate correctly in support of the security requirements.

C.3 The hardware elements of the TOE are as follows:

a) **Data Diode Device**: Part Number FID003.

b) **Power Supply Unit**: This is the power supply unit, 90-264V AC to 5.1V DC.

Procedures for Determining Version of TOE

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.4 Once a Data Diode Device has been received, the following actions should be performed by the administrator:

a) Open the packaging for the Data Diode Device and retrieve the Warning Sheet that provides instructions for examining the Tamper Seal;

b) Recover the faxed checklist that has been sent by the vendor. This checklist provides the Part Number, Device Serial Number, and Seal Serial Number for the delivered Data Diode Device(s);

c) Verify that the tamper seal is not speckled/cut and in accordance with the diagram in section 1.2 of the Administration Manual (ref[10]);

d) Verify that the tamper seal serial number corresponds to the product serial number located on the back of the Data Diode Device case;

e) Check that the corresponding part number for the Data Diode Device on the checklist is **FID003-1.2** and that this number corresponds to the label on the back of the Data Diode Device. **This is the evaluated version**;

f) Initial against the row with the Data Diode Device details;

g) Repeat steps c) through f) for all received Data Diode Devices on the faxed checklist; and

h) Complete the details at the bottom of the checklist and return the list to the vendor's fax number provided on the checklist.

C.5 Once the Data Diode Device has been installed, the following actions can be performed by an Administrator to verify that the Data Diode Device is the evaluated version:

a) Verify that the tamper seal is not speckled/cut and in accordance with the diagram in section 1.2 of the Administration Manual (ref[10]);

b) Check that the corresponding part number label on the rear of the Data Diode Device is labelled **FID003-1.2**. **This is the evaluated version**;

c) The version of any Data Diode Device may be confirmed by contacting Vision Abell and supplying the tamper seal serial number and the serial number on the back of the Data Diode Device.