AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAMME

Certification Report

Certificate Number: 2000/12

Vision Abell Pty Ltd

Interactive Link
NIM001 Version 3.0

Issue 1.0
March 2000

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

The Interactive Link (NIM001 Version 3.0) is a combination of products containing hardware, firmware and software developed by Vision Abell Pty Ltd. It provides the functionality to allow a user to interact with two networks of different classifications from the one desktop computer, while maintaining the confidentiality of the information on the higher classified network.

This report describes the evaluation findings of the Interactive Link NIM001 Version 3.0 product to the ITSEC Assurance Level E6. It also includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product in order to meet the ITSEC E6 level of assurance. It concludes that the product has met the target Assurance Level of E6.

Originator ____________________

Matthew Earley
Certifier
Defence Signals Directorate

Approval ____________________

Andrew M^{C}Cahon
Acting 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 Interactive Link NIM001 Version 3.0 developed by Vision Abell Pty Ltd (hereafter referred to as the Interactive Link). 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 Interactive Link evaluated was part number NIM001, Version 3.0.

1.3 The Interactive Link is a product that allows users to access two differently classified networks from the one desktop computer. A typical Interactive Link installation consists of at least one Keyboard Switch and one Data Diode Device. Various software components are also needed to support the operation of these two devices.

1.4 The Interactive Link consists of the following components:

a) a **Keyboard Switch, FID001, Version 5.0**, and an accessory pack comprising:

i) Power Supply Unit, 90-264V AC to 5.1V DC;
ii) 2 x Network Classification Label Sheets;
iii) 2 x 6-way mini DIN male to male (6-core, 2m) cables;
iv) 1 x 8-way mini DIN male to male (8-core, 2m) cable;
v) Keyboard Switch User Manual (ref [11]).

b) a **Data Diode Device, FID003, Version 1.2,** and an accessory pack comprising:

i) Power Supply Unit, 90-264V AC to 5.1V DC;
ii) Data Diode Device Administration Manual (ref [12]).

c) an Administrator Pack, delivered with the Data Diode Device, comprising:

i) 1 x CDROM (**FIS001**) containing the **Interactive Link Software (including the Red Hat Linux Operating System), Version 2.1**;
ii) 1 x 3.5" boot floppy disk;

iii) Interactive Link Administrator Manual (ref [10]).

1.5 For further details of the evaluated components of the Interactive Link, 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 Interactive Link, 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 November 1998 and March 2000, 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. This 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 Interactive Link 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 Interactive Link product meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtains a copy of the Security Target from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.13 The scope of the evaluation is limited to those claims made in the Security Target. All security related claims in the Security Target were evaluated by Admiral Management Services. A summary of the Security Target is provided in Annex B of this Certification Report

Chapter 2 Security Overview of the Interactive Link

2.1 Potential users are ***strongly*** recommended to read the Security Target (ref [3]). This explains the security functionality of the Interactive Link 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 Pty Ltd.

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 Interactive Link is a combination of products containing hardware, firmware and software developed by Vision Abell (VA). It provides the functionality to allow a user of a secure network (the High Side) the ability to interact with applications on a network of a lower classification (the Low Side), without compromising the confidentiality of the data on the High Side network. The Interactive Link is scalable, depending on the number of users who have a need to access both the High Side and the Low Side networks. The Interactive Link consists of at least one Keyboard Switch, one Data Diode Device and supporting software.

2.4 The Data Diode Device allows data to pass in only one direction. In the Interactive Link, it receives data from the Low Side network and passes it to the High Side network. Once installed, the Data Diode Device is intended to operate transparently to users on either the Low Side or High Side network and without the need for any administration. No data can pass from the High Side network to the Low Side network through the Data Diode Device.

2.5 The Keyboard Switch connects between the user's desktop computer (connected to the High Side network) and SUN or PS/2 keyboard and mouse devices. It also connects to the Low Side network. It provides a trusted switching function that allows the user to direct keyboard and mouse data either to applications on the Low Side network or to the user's desktop computer that is connected to the High Side network. At all times while it is powered on, the Keyboard Switch provides a visual indication to the user as to which network (Low or High) the Keyboard Switch is currently connected. Additionally, whenever the user switches networks (achieved by pressing a corresponding button), an audible indication is provided that the switch has occurred successfully.

2.6 The Interactive Link software resides on either two or four servers. In the two-server configuration, one server is connected between the Low Side network and the Data Diode Device while the other is connected between the Data Diode Device and the High Side network. In the four-server configuration two servers reside on either side of the Data Diode Device. The server hardware is not provided with the TOE.

2.7 The Interactive Link software provides communications and network support to allow users to interact with applications on the Low Side network servers, when connected to the Low Side network through the Keyboard Switch, and display application windows on their desktop. Users can also cut and paste data from Low to High windows, and transfer files from the Low Side network servers to the High Side network. However, due to the Interactive Link security enforcing functions and intended environment, no information can be transferred from the High Side network to the Low Side network.

2.8 The Interactive Link provides a single security objective to keep information of the High Side network confidential from the Low Side network. In doing so, the Interactive Link implements three Security Enforcing Functions (SEFs) in hardware. These are a Data Diode Function, a Data Path Switch Function and an Indication Function, and are provided by the Data Diode Device and the Keyboard Switch. The Interactive Link software does not contribute to achieving the security objective of the Interactive Link.

2.9 More detailed information on the Interactive Link SEFs can be found in the Security Target for the Interactive Link product (ref [3]), and in Appendix B of this report.

Documentation

2.10 Prospective users of the Interactive Link are ***strongly*** recommended to obtain a copy of the Data Diode Device Certification Report (ref [19]). This product has undergone a separate evaluation by the AISEP to an E6 level of assurance. The Certification Report contains important information about the Data Diode Device that must be considered by potential customers and administrators of the Interactive Link.

2.11 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, the Keyboard Switch User Manual (ref[11]), the Interactive Link Administrator Manual (ref [10]), and the Data Diode Device Administration Manual (ref [12]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of the Interactive Link 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 (SEF) 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 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 Functions 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 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 and separated into two security enforcing components (the Keyboard Switch and the Data Diode Device) and two security irrelevant components (the High and Low Side Interactive Link Servers).

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 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 and security relevant 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 SEFs identified in the Detailed Design are identifiable and correct in the hardware drawings, and consistent with the formal specification of the SEFs 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 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 E6 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 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.

3.14 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Development Environment.

Correctness – Operation

3.15 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.

3.16 The evaluators determined that the operational documentation (refs [10,11,12]) explained the operation of the SEFs relevant to the administrator of the TOE and explained how to operate the TOE in a secure manner.

3.17 The evaluators determined that the startup and operation documentation (refs [10,11,12]) explained the procedures for secure startup and operation of the TOE.

3.18 The evaluators determined that the assembly and delivery documentation (refs [13,14,15]) explained the delivery arrangements from the development environment to the customer site, and that the generation of the TOE for delivery was explained.

3.19 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

3.20 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

3.21 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.

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

Binding Analysis

3.23 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.

3.24 The evaluators reported an unresolved issue in the analysis of covert channels relating to the existence of a potential covert channel identified by the developers. Although the bandwidth of this potential channel was not measured through testing, the evaluator's analysis showed that it is less than two bits per second. In addition, the existence of this channel relies on the execution of malicious code on the High Side network, and the continuous activity of user acting in response to the malicious software. However, this covert channel is mitigated by the environmental assumptions about the protection of the High Side network environment which would ensure that appropriate software procurement policies are followed to minimise the risk of malicious software, and its detection by virus scanners or other appropriate mechanisms.

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

Strength of Mechanisms Analysis

3.26 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.

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

Construction Vulnerability Assessment

3.28 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 evaluators reviewed the developer's Construction Vulnerability Assessment, and also performed their own assessment to find potential vulnerabilities in the TOE. The evaluators were unable to find any vulnerabilities in construction of the TOE. The assessment showed that a number of single point hardware failures in the TOE were identified as potential vulnerabilities in the operation of the TOE. Further, testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities due to its construction.

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

Effectiveness – Operation

3.30 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

3.31 The evaluators found that the TOE could not be configured or used in a manner which was insecure but which an Administrator or end-user would believe to be secure. Further, the evaluators found that the TOE could be installed and used securely using only the User and Administration Manuals (refs [10,11,12]) as guidance, and that all possible failure modes were adequately documented, along with their effects.

3.32 The evaluators reported an unresolved issue in the Ease of Use Analysis. This issue is related to the possible mis-configuration of the TOE due to incorrect installation of the classification labels affixed to the front fascia of the Keyboard Switch, and incorrect configuration of the non-security enforcing Interactive Link components.

3.33 The possibility of failure of the TOE due to this mis-configuration was not fully considered in the developer's Ease of Use Analysis, however the evaluator's own analysis (supported by the evaluator's penetration testing) showed that any mis-configuration of this type would not lead to insecure operation of the TOE which would not be obvious to the administrator or end user. Based upon this analysis and testing, the certifiers judge that this issue does not affect the overall assurance or security of the TOE.

3.34 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 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 several vulnerabilities in the operation of the TOE that encapsulated all modes of failure identified in the Construction Vulnerability Assessment. 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 met the ITSEC E6 requirements for the Operational Vulnerability Assessment.

Specific Functionality

3.37 The Security Enforcing Functions (SEFs) provided by the Interactive Link are specified in section 4.2 of the Security Target (ref [3]) and summarised in Appendix B of this report.

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

Discussion of Unresolved Issues

3.39 At the conclusion of the evaluation process, two issues identified by the evaluators remained unresolved. These issues have been identified and discussed in previous sections of this chapter and have been suitably addressed in the certification process. As a result, there are no remaining unresolved issues following certification of the Interactive Link.

General Observations

3.40 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.

3.41 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.

3.42 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, the Australasian Certification Authority has determined that the Interactive Link has met the requirements of the ITSEC E6 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 3.0 of the product. This certificate is only valid when the Interactive Link 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 Interactive Link should only be used in accordance with the intended environment described in section 3.4 of the Security Target (ref [3]), including consideration of all physical, personnel and procedural security measures. Further, it is recommended that the Interactive Link 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.

4.5 Please note that recommendations for the Data Diode Device have been included in this chapter. This does not remove the responsibility for potential customers and administrators of the Interactive Link to obtain a copy of the Data Diode Device Certification Report (ref [19]). The Data Diode Device Certification Report contains other important information that must be considered and used as a supplement to the findings in this report.

Installation of the Interactive Link

4.6 There is a risk that an End-User could incorrectly install the cabling and/or classification labels of the TOE causing a user to enter High Side information onto the Low Side Network. **To reduce this risk, the Interactive Link should only be installed by an appropriately trained and authorised Administrator in accordance with the Interactive Link Keyboard Switch User Manual (ref [11]), the Interactive Link**

Administrator Manual (ref [10]), and the Data Diode Device Administration Manual.

4.7 The Interactive Link software package includes a tailored version of the Red Hat Linux operating system. Administrators need to be aware that the Interactive Link software is integrated with the Red Hat Linux operating system. **Under no circumstances should another version of the Linux or Unix operating system be used in place of the supplied version.**

4.8 The Interactive Link requires several configuration files (e.g. /etc/hosts) that require the administrator to add the IP address and/or the name of every Keyboard Switch on the network. Some of these files are common to both the High and Low Side controllers. Section 5.5 of the Interactive Link Administrator Manual (ref [10]) provides a warning to the administrator not to use any High Side information in the naming convention of Keyboard Switches. **Administrators should ensure that the appropriate naming conventions are used for Keyboard Switches. Furthermore, all notes and warnings concerning the configuration process for the Interactive Link software must be fully understood prior to system installation.**

Location of the Data Diode Device and Data Receiver

4.9 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**.

Location of the Keyboard Switch

4.10 The Keyboard Switch requires connection to a *High Side computer* and a *Low Side network*. The Keyboard Switch **must** be located in the same security environment as the *High Side computer* and ideally located beneath the user's display. **In any case the visual indicators must be clearly in view at all times. System Administrators should ensure that users do not obstruct their view of the trusted indicators at any time when operating the TOE.**

Tamper Seal and Cable Integrity

4.11 Administrators should locate the Keyboard Switch such that the tamper seal is clearly visible at all times. 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 Data Diode Device Administration Manual (ref [12]) and the Keyboard Switch User Manual (ref [11]). A regular inspection procedure should be incorporated into the site or system security plan.

The Administrator or an End-User should immediately report any discovery of damage or tamper to their appropriate security authority and the TOE should be removed.

4.12 When inspecting the tamper seal on the Keyboard Switch, administrators or an End-User should also check the cabling connections from the Keyboard Switch to the *High Side computer* when checking the integrity of the tamper seal, to ensure that the Keyboard Switch is correctly connected with the supplied cables.

4.13 When inspecting the tamper seal on the Data Diode Device, 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.

Requirements for Additional Tamper Seals

4.14 The Keyboard Switch allows System Administrators to install appropriate classification labels when installing the device. **Administrators should note that the Keyboard Switch does not counter any threats of an attacker changing or reversing the classification labels on the device.** In higher security environments it is ***strongly*** recommended that the front shield be sealed with an appropriate tamper seal once an Administrator has installed the TOE. It is recommended that this **additional tamper seal be placed on the top of the front panel of the Keyboard Switch, by an Administrator after the classification labels are installed, such that the seal is centrally located on the front panel and covers the join between the front shield and the front panel of the TOE (see Figure 1)**.

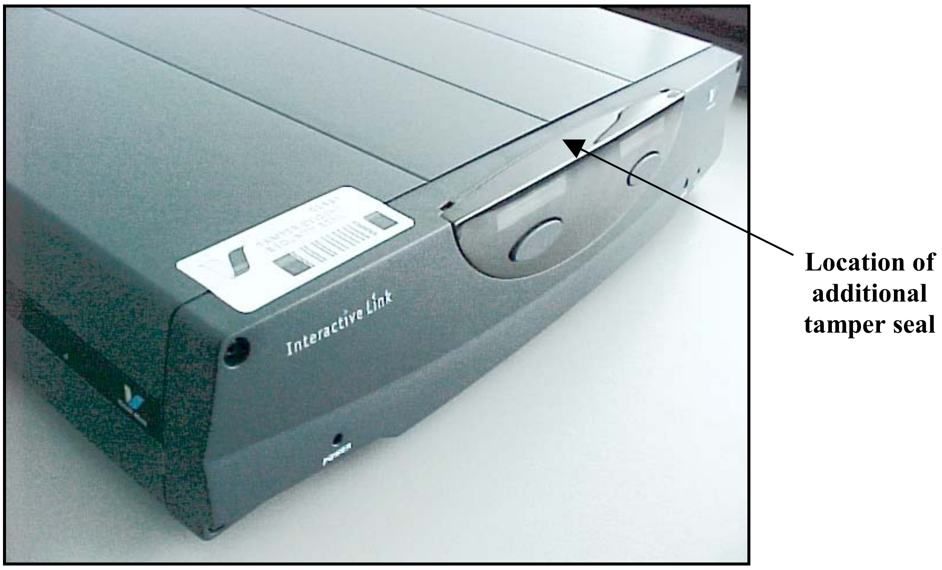

Figure 1 - Additional Tamper Seal Location for High Security Environments

4.15 The appropriate security authority for accrediting the site where the TOE is installed should be able to recommend tamper seals that are appropriate for the operating environment. **Under no circumstances should the existing tamper seal located on the top of the front panel ever be removed and/or replaced.**

Protocol Considerations

4.16 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.

Integrity and Availability of High Side Network

4.17 **Administrators should note that the Interactive Link 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 for the Data Diode Device

4.18 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.

4.19 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* be plugged, or disabled, to prevent inadvertent connection of the Data Diode Device in the reverse direction.** Please note that the input socket of the data transmitter requires a loopback cable connecting to a secondary network interface card on the Low Side Data Diode Server. **The input socket of the secondary network interface card should also be plugged to reduce the possibility of a High to Low bypass of the Data Diode Device.**

User Training

4.20 Administrators should ensure that all users are appropriately trained in the operation of the Keyboard Switch. In particular, all users should be made aware of their responsibilities to monitor the integrity of the tamper seal(s) affixed to the product.

Further, all users should be made familiar with the **Troubleshooting Guide** in the Keyboard Switch User Manual (ref [11]) as it is essential that a user can detect abnormal operation of any of the security features of the product. **If at any time a user detects an abnormality with any of the security features of the product, they should immediately report the problem to the System Administrator or appropriate Security Authority and stop using the product**. In the case of abnormal function, the Keyboard Switch should immediately be returned to the manufacturer in accordance with the Troubleshooting Guide in the Keyboard Switch User Manual (ref [11] section 4).

Guidance for Purchasers - Delivery Procedures

4.21 Purchasers of the Interactive Link should note that the delivery procedures must be followed to ensure the authenticity and integrity of the delivered TOE components. 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 Interactive Link 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. **When taking delivery of the TOE, if the tamper seal shows any sign of damage and/or tamper the recipient should immediately contact the product vendor and the appropriate accreditation authority to report the incident. Under no circumstances should the product be used.**

4.22 If the Interactive Link 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 Data Diode Device Administration Manual (ref [12]) and the Keyboard Switch User Manual (ref [11]). If for any reason, an Interactive Link component needs to be returned to the manufacturer, the administrator(s) should contact the product vendor for instructions of how to return the equipment.

Guidance for Purchasers - Residual Risk of Covert Channels

4.23 Given that the Interactive Link protects the confidentiality of information on the High Side network from the Low Side network, covert channels are a consideration for prospective purchasers. **The evaluation determined that two exploitable ‘user assisted’ covert channels exist within the Interactive Link. The evaluators measured the maximum bandwidth of the covert channels at five bits per second each.** These ‘user assisted’ covert channels require the interaction of a malicious user with the Interactive Link. Therefore, **if the Interactive Link 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.**

High and Low Side Windows

4.24 The Interactive Link Low Side desktop is represented within a High Side window. To reduce the risk that a user may inadvertently enter High Side information while connected to the Low Side network, it is recommended that certain restrictions be placed on the window(s) that is interacting with the Low Side network. This may take the form of restricting the size of the window, or significantly altering the colouring schemes used by the High and Low Side windows. **Further, in high security environments, the ability to modify the properties of the windows that interact with the Low Side should be restricted to that of the System Administrator(s).**

Guidance for Purchasers – Peripheral Products

4.25 The Interactive Link does not counter the threat of a 'non-standard' peripheral device storing information entered by a user when in High mode and later forwarding that information to the Low Side network when in Low mode. Purchasers of keyboard and mouse peripheral products that will be connected to the Keyboard Switch should **ensure that these products conform to the PS/2 or SUN standard**.

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] Interactive Link Security Target
Vision Abell Pty Ltd.
Issue 6.0, 1st March 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] Interactive Link Evaluation Technical Report
Admiral Management Services
Issue 1.1, March 2000.
(EVALUATION-IN-CONFIDENCE, RESTRICTED, COMMERCIAL-IN-CONFIDENCE)

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

[10] Interactive Link Administrator Manual
Vision Abell Pty Ltd
Issue 5.0
Part Number SUG001-5

[11] Interactive Link Keyboard Switch User Manual
Vision Abell Pty Ltd
Issue 5.0
Part Number SUG002-5

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

[13] KBS Assembly Procedure
Vision Abell Pty Ltd
96162D01990101, Issue 3.1, 1st November 1999

[14] Interactive Link Administrator Pack Assembly Procedure
Vision Abell Pty Ltd
96162D01990104, Issue 1.0, 9th July 1999

[15] Infosec Division Work Instruction for Delivery Procedures for Interactive Link Components
Vision Abell Pty Ltd.
Infosec/WI/060201, Issue 1.0, 11th November 1999
(COMMERCIAL-IN-CONFIDENCE)

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

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

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

[19] Certification Report
Vision Abell Pty Ltd Data Diode Device FID003 Version 1.2
Defence Signals Directorate
Issue 1.0, November 1999

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 Interactive Link has the following IT security objective:

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

Intended Method of Use and Intended Environment

B.3 The Intended Method of Use for the Interactive Link is:

a) The user may interact with information and applications located on the High Side Network, when the high button of the Keyboard Switch is pressed placing the Interactive Link in high mode. In this mode, the keyboard and mouse data is passed via the Keyboard Switch to the High Side window server to interact with the applications on the High Side Network.

b) The user may interact with information and applications located on the Low Side Network, when the low button of the Keyboard Switch is pressed placing the Interactive Link in low mode. In this mode, the keyboard and mouse data are passed to the Low Side application server to interact with applications on the Low Side Network. The application output is passed via Data Diode Device to the High Side window server.

c) In low mode, the user can cut and copy text information into the Low Side Network clipboard, and transfer this information via the Data Diode Device to the High Side Network, so that it can be used by applications residing on the High Side Network.

d) In low mode, files may be copied and transferred from the Low Side Network to the High Side Network via the Data Diode Device.

e) Applications on the Low Side and High Side Networks may be displayed simultaneously on the user's window server. Application data from the Low Side Network is transferred to the High Side Network via the Data Diode Device for display on the user's High Side window server.

f) The user, depending on the mode of the Keyboard Switch, can modify the dimensions of all windows.

g) When the user terminates their Low Side session, the entire Interactive Link session is also terminated, along with the Low and High Side Network Interactive Link applications.

B.4 The Intended Environment for the Interactive Link is:

a) The Interactive Link shall be operated in an environment that meets the requirements of SECMAN3 (ref [16]), ACSI33 (ref [17]) or ASSRO Supplement 1 (ref [18]).

b) The Interactive Link shall be operated and stored in accordance with the requirements of the network with the highest classification.

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

d) The trusted device casings 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 operator will be responsible for monitoring the tamper seal on the Keyboard Switch. The ISSO or the System Administrator will be responsible for monitoring the tamper seal on the Data Diode Device.

e) The system management staff shall install the Interactive Link in accordance with the administration documentation. The appropriate security authority shall accredit the installation and procedures for the Interactive Link.

f) The Interactive Link 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 Interactive Link 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 an Interactive Link.

g) Appropriate equipment hardware procurement policies are to be followed to minimise the risk of installing malicious hardware and/or software.

h) 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 Functions (SEFs) are provided by the Interactive Link:

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, applications or users on the Low Side Network cannot get access to information on the High Side Network via the Data Diode Device in accordance with the security objective.

B.7 SF2:

Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Network (denoted as "High Mode") or the Low Side Network (denoted as "Low Mode"), according to the mode selected by the User. This function ensures that keyboard and mouse data are directed to its intended destination as selected by the user. This function prevents data flowing from the High Side Network and the Low Side Network into the keyboard and mouse.

B.8 SF3:

Indication Function: To indicate the current mode to the user. This function ensures that the user is aware of the current mode and thus the destination of keyboard and mouse data. This function also indicates a successful change of mode to the user.

Appendix C Contents of Distribution Package

Configuration for Evaluation

C.1 The evaluation was conducted on Vision Abell's Interactive Link, part number NIM001 Version 3.0. The hardware and software components of the Interactive Link have been identified below.

Hardware

C.2 There are two hardware components in the Interactive Link. They are the Keyboard Switch and the Data Diode Device.

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 Keyboard Switch are as follows:

a) **Keyboard Switch:** Part number FID001, Version 5.0;

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

c) **6-way mini DIN male to male (6-core, 2m) cables:** There are two of these for connecting the PS/2 keyboard and mouse receptacles of the Keyboard Switch to the user's workstation;

d) **8-way mini DIN male to male (8-core, 2m) cable:** There is one cable for connecting the SUN keyboard and mouse receptacle of the Keyboard Switch to the user's workstation;

C.5 The hardware elements of the Data Diode Device are as follows:

a) **Data Diode Device:** Part number FID003, Version 1.2;

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

Software

C.6 The software elements of the Interactive Link are as follows:

a) 1 x CDROM (part number **FIS001**) containing the **Interactive Link Software (including the Red Hat Linux Operating System), Version 2.1**.

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.

These instructions refer to all of the components that form the Interactive Link (i.e. the Keyboard Switch, the Data Diode Device and the Interactive Link software). **Please note that the Interactive Link software and associated documentation are delivered with the Data Diode Device.**

C.7 Once an Interactive Link has been received, the following actions should be performed by the administrator:

a) Open the packaging for the Keyboard Switch or 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 Keyboard Switch(es) or the Data Diode Device(s). The Part Number and Version number should also be supplied for the CD-ROM that contains the Interactive Link software;

c) Verify that the tamper seal is not speckled/cut and is in accordance with the diagram in section 1.2 of the Keyboard Switch User Manual (ref [11]) or section 1.2 of the Data Diode Device Administration Manual (ref [12]);

d) Verify that the tamper seal serial number corresponds to the product serial number located on the back of the Keyboard Switch or Data Diode Device, in accordance with the faxed checklist;

e) Check that the corresponding part numbers are **FID001-5.0** for the Keyboard Switch, **FID003-1.2** for the Data Diode Device, and **FIS001-2.1** for the Interactive Link software on the faxed checklist. These numbers must correspond to the labels on the back of the Keyboard Switch and Data Diode Device, and on the label affixed to the CD-ROM for the Interactive Link software. **These are the evaluated versions**;

f) Initial against the row with either the Keyboard Switch, Data Diode Device or Interactive Link software details;

g) Repeat steps c) through f) for all received Keyboard Switches, Data Diode

Devices or Interactive Link software 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.8 Once the Interactive Link has been installed, the following actions can be performed by an Administrator to verify that the Interactive Link components are the evaluated versions:

a) Verify that the tamper seal is not speckled/cut and is in accordance with the diagram in section 1.2 of the Keyboard Switch User Manual (ref [11]) or the Data Diode Device Administration Manual (ref [12]);

b) Check that the corresponding part numbers on the back of the devices are **FID001-5.0** for the Keyboard Switch and **FID003-1.2** for the Data Diode Device. **These are the evaluated versions**;

c) The version of any Keyboard Switch or 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 respective device(s).

d)