AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAMME

Certification Report

Certificate Number: 2000/11

Vision Abell Pty Ltd

Interactive Link Multiple Computer Switch FID004 Version 2.0

Issue 1.0
March 2000

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

The Vision Abell Interactive Link Multiple Computer Switch (IL-MCS) is a hardware/firmware device that provides functionality to allow a user to interact with two personal computers of different classifications, via a common set of input and output devices, while maintaining the confidentiality of the information on the higher classified computer.

This report describes the evaluation findings of the Vision Abell Interactive Link Multiple Computer Switch FID004 Version 2.0 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 its 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 _____

Peter Lilley
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 Vision Abell Interactive Link Multiple Computer Switch FID004 Version 2.0 (hereafter referred to as the Multiple Computer Switch). 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 Multiple Computer Switch evaluated was FID004, Version 2.0.

1.3 The Multiple Computer Switch is a hardware/firmware product. There are no software components associated with the product.

1.4 The Multiple Computer Switch consists of:

a) a Multiple Computer Switch;

b) a Multiple Computer Switch Accessory Pack containing:

(i) Power Supply Unit, 90-264V AC to 5V DC;

(ii) 2 x Classification Label Sheets;

(iii) 4 x Cables, 6-way mini DIN male to male (6-core, 2m); and

(iv) 2 x Cables, 15-pin VGA D-Type male to female (6+3 coax, twin ferrites, 2m).

c) a combined Multiple Computer Switch User and Administration Manual.

1.5 For further details of the evaluated components of the Multiple Computer Switch, 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 Multiple Computer Switch, 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 February 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. 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 Multiple Computer Switch 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 Multiple Computer Switch 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. Everything claimed in the Security Target was 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 IL-MCS

2.1 Potential users are ***strongly*** recommended to read the Security Target (ref [3]). This explains the security functionality of the Multiple Computer Switch 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 Multiple Computer Switch is a hardware and firmware product designed by Vision Abell (VA). It provides the functionality to allow a user to work with two personal computers of different classifications without compromising the confidentiality of the data on the higher classified computer, while using a single PS/2 keyboard, PS/2 mouse and a VGA capable monitor. Keyboard and mouse data is directed through the Multiple Computer Switch to the selected computer and video output from the selected computer is directed to the common display monitor.

2.4 In its evaluated configuration the Multiple Computer Switch is connected between two personal computers of different classifications, with operating systems capable of handling PS/2 keyboard and mouse data and providing VGA monitor output. A common keyboard and mouse are connected to the Multiple Computer Switch to allow the user to send data to the selected personal computer, and a common monitor is connected to the Multiple Computer Switch to receive video output from the selected personal computer. Users select the personal computer they wish to interact with by pressing a button on the front of the Multiple Computer Switch. At all times, the user is provided with visual feedback of which personal computer they are interacting with through a set of trusted visual and audible indicators.

2.5 The Multiple Computer Switch provides a single security objective to keep information of the High Side Computer confidential from the Low Side Computer. In doing so, the Multiple Computer Switch implements three Security Enforcing Functions (SEFs) in hardware. These are a Data Path Switch Function, a Video Path Switch Function and an Indication Function.

2.6 More detailed information on the Multiple Computer Switch SEFs can be found in the Security Target for the Multiple Computer Switch 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 Multiple Computer Switch User and Administration Manual (ref [10]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of the Multiple Computer Switch 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 as and separated into two security enforcing components, one security relevant component and two security irrelevant 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 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 was 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 (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.

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

3.18 The evaluators determined that the assembly and delivery documentation (ref [11,12]) explained the delivery arrangements from the development environment to the customer site, and that the generation of the TOE for delivery was explained.

3.19 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 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

3.25 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.

3.26 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

3.27 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, in fact, covered 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.

3.28 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

3.29 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

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

3.31 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

3.32 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 five 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 corrected or countered by other measures.

3.33 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

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

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

Discussion of Unresolved Issues

3.36 At the conclusion of the evaluation there were no unresolved issues requiring the consideration of the certifiers.

General Observations

3.37 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.

3.38 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.

3.39 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 Multiple Computer Switch has met the requirements of the ITSEC E6 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 2.0 of the product. This certificate is only valid when the Multiple Computer Switch 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 Multiple Computer Switch 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 Multiple Computer Switch 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.

Installation of the Multiple Computer Switch

4.5 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 Computer. **To reduce this risk, the Multiple Computer Switch should only be installed by an appropriately trained and authorised Administrator in accordance with the User and Administration Manual (Ref[10]) and taking note that the orientation of the video interfaces and the keyboard/mouse interfaces are opposite.**

Alternative Installation Procedure

4.6 Given the orientation of the connectors on the back of the Multiple Computer Switch, and the common cabling for both the High Side Computer and the Low Side Computer, there is an increased risk of installing cabling incorrectly that may cause an end-user to enter High Side information onto the Low Side Computer. **To reduce this risk in high security environments, it is recommended that Administrators use the following alternative installation procedure when installing the Multiple Computer Switch to reduce the risk of an incorrect installation (Note: Administrators will need to consult Figure 1-4 of the User and Administration Manual (Ref[10] when using this procedure):**

(i) Read section 2.3 and section 2.3.1 of the User and Administration Manual (Ref [10]). Replace section 2.3.2, section 2.3.3 and section 2.3.4 of the User and Administration Manual (ref[10]) with the following procedure;

(ii) Ensure that both the High Side Computer and the Low Side Computer have been shutdown and powered off in accordance with the manufacturer's instructions;

(iii) Ensure that the Multiple Computer Switch is powered off;

Installation of Common Peripheral Devices

(iv) Connect the PS/2 keyboard and PS/2 mouse devices that will be used as the common input devices for the High Side Computer and the Low Side Computer to the Keyboard receptacle [3] and the Mouse receptacle [4] on the back panel of the Multiple Computer Switch as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(v) Connect the display monitor that will be used to display the video output from both the High Side Computer and Low Side Computer to the Monitor receptacle [9] on the back panel of the Multiple Computer Switch as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

Connection of Low Side Computer and Verification

(vi) Connect one of the 6-way cables from the Low Computer Keyboard Receptacle [1] on the back of the Multiple Computer Switch to the PS/2 Keyboard input socket on the Low Side Computer as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(vii) Connect one of the 6-way cables from the Low Computer Mouse Receptacle [2] on the back of the Multiple Computer Switch to the PS/2 Mouse input socket on the Low Side Computer as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(viii) Connect one of the 15-pin cables from the Low Side Computer Video Socket to the Low Computer Video Receptable [8] on the back of the Multiple Computer Switch as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(ix) Verify that all Low Computer Receptacles [1], [2] and [8] (Ref[10], Figure 1-4, page 1-7) on the back of the Multiple Computer Switch are now connected to the Low Side Computer;

(x) Verify that the Keyboard and Mouse Receptacles [3] and [4] , and the Monitor receptacle [9] (Ref[10], Figure 1-4, page 1-7) on the back of the Multiple Computer Switch are now connected to the common peripheral devices;

(xi) Connect the 5V DC plug pack (power supply) to the power receptacle [7] on the back of the Multiple Computer Switch as shown in the User and Administration Manual (ref[10], Figure 1-4, page 1-7);

(xii) Connect the power supply to the mains outlet and turn the power on. The Multiple Computer Switch must start in High Mode. (i.e. The High Side Classification Label should be illuminated). If this does not occur DO NOT USE THE DEVICE and refer to the troubleshooting section on the User and Administration Manual (Ref[10], Section 4);

(xiii) Change the Multiple Computer Switch into Low Mode by pressing the Low Side Classification Button. (i.e. the Low Side Classification Label should be illuminated and an audible beep will sound). If this does not occur DO NOT USE THE DEVICE and refer to the troubleshooting section on the User and Administration Manual (Ref[10], Section 4);

(xiv) Apply power to the Low Side Computer (and the monitor if appropriate) and wait for the boot sequence to complete. Verify that the video output during the boot sequence is displayed on the monitor;

(xv) Check that the Keyboard and Mouse can be used to interact with the Low Side Computer by typing characters and using the mouse;

(xvi) **The Low Side Computer has now been installed correctly;**

Connection of High Side Computer and Verification

(xvii) Shutdown the Low Side Computer and power off in accordance with the manufacturer's instructions;

(xviii) Remove power to the Multiple Computer Switch by turning off power at the mains outlet;

(xix) Connect one of the 6-way cables from the High Computer Keyboard Receptacle [5] on the back of the Multiple Computer Switch to the PS/2 Keyboard input socket on the High Side Computer as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(xx) Connect one of the 6-way cables from the High Computer Mouse Receptacle [6] on the back of the Multiple Computer Switch to the PS/2 Mouse input socket on the High Side Computer as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(xxi) Connect one of the 15-pin cables from the High Side Computer Video Socket to the High Computer Video Receptable [10] on the back of the Multiple Computer Switch as shown in the User and Administration Manual (Ref[10], Figure 1-4, page 1-7);

(xxii) Verify that all High Computer Receptacles [5], [6] and [10] (Ref[10], Figure 1-4, page 1-7) on the back of the Multiple Computer Switch are now connected to the High Side Computer;

(xxiii) Connect the 5V DC plug pack (power supply) to the power receptacle [7] on the back of the Multiple Computer Switch as shown in the User and Administration Manual (ref[10], Figure 1-4, page 1-7);

(xxiv) Connect the power supply to the mains outlet and turn the power on. The Multiple Computer Switch must start in High Mode. (i.e. The High Side Classification Label should be illuminated). If this does not occur DO NOT USE THE DEVICE and refer to the troubleshooting section on the User and Administration Manual (Ref[10], Section 4);

(xxv) Apply power to the High Side Computer (and the monitor if appropriate) and wait for the boot sequence to complete. Verify that the video output during the boot sequence is displayed on the monitor;

(xxvi) Check that the Keyboard and Mouse can be used to interact with the High Side Computer by typing characters and using the mouse;

(xxvii) **Both the High and Low Side Computers have now been installed correctly;**

(xxviii) Shutdown the High Side Computer and power off in accordance with the manufacturer's instructions. Refer to the operating instructions (Ref[10], Section 3, page 3-1) of the User and Administration Manual for user operation;

Location of the Multiple Computer Switch

4.7 The Multiple Computer Switch requires connection to a *High side personal computer* and a *Low side personal computer*. The Multiple Computer Switch **must** be located in the same security environment as the *High side personal 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

4.8 Administrators should locate the Multiple Computer 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 User and Administration Manual (ref [10]). 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.** Administrators or an End-User should also check the cabling connections for the Multiple Computer Switch to the *High Side personal computer* and the *Low Side personal computer* when checking the integrity of the tamper seal, to ensure that the Multiple Computer Switch is correctly connected with the supplied cables.

Requirements for Additional Tamper Seals

4.9 The Multiple Computer Switch allows System Administrators to install appropriate classification labels when installing the TOE. **Administrators should note that the Multiple Computer Switch does not counter any threats of an attacker changing or reversing the classification labels on the TOE.** In higher security environments it is ***strongly*** recommended that the front shield (as described in the User and Administration Manual (ref[10]) 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 Multiple Computer 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)**.

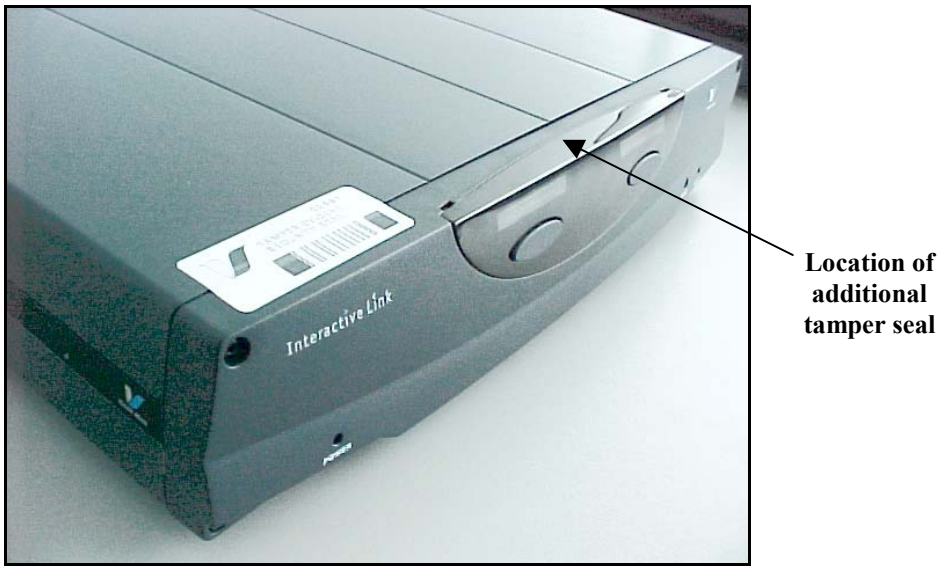

Figure 1 - Additional Tamper Seal Location for High Security Environments

4.10 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.**

High and Low Side Computer Requirements

4.11 To reduce the risk that a user may inadvertently enter high side information while connected to the Low Side personal computer, it is recommended that significantly different colour schemes, wallpaper and screensavers be used on the High Side and the Low Side Computers. **Further, in high security environments, the ability to modify the desktop settings should be restricted to that of the System Administrator(s).**

4.12 Administrators should locate the High and Low Side Computers such that they are oriented in the same manner as the classification labels. **Since the Low Side classification label is on the left hand side of the IL-MCS when looking at the front panel, the Low Side Computer should be positioned on the left hand side of the IL-MCS when looking at the front panel.** Further, in higher security environments it is recommended that the High and Low Side Computers should be appropriately separated to reduce the risks of any electromagnetic leakage from the High Side Computer to the Low Side Computer. System accreditors should consider the separation of the High and Low Side Computers when accrediting installations of the Multiple Computer Switch.

4.13 Care should be taken when connecting the power source for the common monitor. It is not recommended that Administrators use 'piggy-back' type power connections that are sometimes located on the back of computer housings. It is recommended that the monitor

be powered directly from a separate main outlet to reduce the risk of electromagnetic leakage.

4.14 If the High and Low Side Computers contain removable hard drives, Administrators should note that there is a risk of inserting the higher classified hard drive in the Low Side Computer, when the same type of hard drive cradle are used in both the High and Low Side Computers. It is recommended **that all removable hard drive are appropriately labelled and, if possible, different hard drive cradles are used on the High and Low Side Computers.**

4.15 Administrators should disable floppy drive access to both the High and Low Side Computers to prevent the possibility that a user could transfer High Side information to the Low Side or vice versa. **Administrators should consider other appropriate evaluated products or mechanisms for controlling the transfer of information from the Low Side to the High Side Networks or Computers.**

User Training

4.16 Administrators should ensure that all users are appropriately trained in the operation of the Multiple Computer 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 User and Administration Manual (Ref [10]) 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 Multiple Computer Switch should immediately be returned to the manufacturer in accordance with the Troubleshooting Guide in the User and Administration Manual (Ref [10] section 4).

Guidance for Purchasers - Delivery Procedures

4.17 Purchasers of the Multiple Computer Switch 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 Multiple Computer Switch 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 Australasian Certification Authority to report the incident. Under no circumstances should the product be used.**

4.18 If a Multiple Computer Switch 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]). If for any reason, a Multiple Computer Switch needs to be returned to the manufacturer, the administrators should contact the product vendor for instructions of how to return the equipment.

Guidance for Purchasers - Residual Risk of Covert Channels

4.19 Given that the Multiple Computer Switch protects the confidentiality of information on the High Side Computer from the Low Side Computer, covert channels are a consideration for prospective purchasers. **The evaluation determined that a single exploitable 'user assisted' covert channel exists within the Multiple Computer Switch. The evaluators measured the maximum bandwidth of the covert channel at 5bits/second.** A 'user assisted' covert channel requires the interaction of a malicious user with the Multiple Computer Switch. Therefore, **if the Multiple Computer Switch is only used within its intended operational environment (Ref [3]), then this covert channel is unlikely to be exploitable within that operational environment, due to the appropriate security clearance and training of staff.**

Guidance for Purchasers – Peripheral Products

4.20 The Multiple Computer Switch 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 Computer when in Low mode. Purchasers of keyboard and mouse peripheral products that will be connected to the Multiple Computer Switch should **ensure that these products conform to the PS/2 standard**. Purchasers of the display monitor that will be connected to the Multiple Computer Switch should **ensure that the monitor is capable of accepting VGA input signals**. **Note that the Plug and Play features of current video monitors will not function through the Multiple Computer Switch.**

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 Multiple Computer Switch Security Target
Vision Abell Pty Ltd.
Issue 3.0, 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] Multiple Computer Switch Evaluation Technical Report
Admiral Management Services
Issue 1.1, March 2000.
(EVALUATION-IN-CONFIDENCE, RESTRICED, COMMERCIAL-IN-CONFIDENCE)

[9] Interactive Link Multiple Computer Switch Formal Policy and Architecture
Defence Science and Technology Organisation

Version 2.0, 10th December 1999.

[10] Interactive Link User and Administration Manual
Vision Abell Pty Ltd
Issue 3.0
Part Number SUG003-3

[11] MCS Assembly Procedure
Vision Abell Pty Ltd
96162D01990103, Issue 3.1, 28th October 1999

[12] 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)

[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 Multiple Computer Switch has the following IT security objective:

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

Intended Environment and Intended Method of Use

B.3 The Intended Method of Use for the Multiple Computer Switch is:

a) The Multiple Computer Switch is connected between two personal computers of different classifications (a High Side Computer and a Low Side Computer). A user can connect a set of shared peripheral devices (a keyboard, mouse and display) to either the High Side Computer or the Low Side Computer (but not both at the same time) by pressing a button on the Multiple Computer Switch. Pressing the High Side button sets the Multiple Computer Switch to High Mode and the user can interact with the High Side Computer. Pressing the Low Side button sets the Multiple Computer Switch to Low Mode and the user can interact with the Low Side Computer.

B.4 The Intended Environment for the Multiple Computer Switch is:

a) The Multiple Computer Switch 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 Multiple Computer Switch shall be operated and stored in accordance with the requirements of the computer with the highest classification.

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

d) The Multiple Computer Switch 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 end-user shall be responsible for monitoring the Multiple Computer Switch tamper seal.

e) The system management staff shall install the Multiple Computer Switch in accordance with the administration documentation. The appropriate security authority shall accredit the installation of the Multiple Computer Switch.

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

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 Multiple Computer Switch:

Data Path Switch SEF

B.6 SF1:

Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer or the Low Side Computer, 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 Computer and the Low Side Computer into the keyboard and mouse.

B.7 SF2:

Video Path Switch Function: To transfer data from either the High Side Computer or the Low Side Computer to the monitor, according to the mode selected by the User. This function ensures that video data is transferred from the source to either the High Side Computer or the Low Side Computer to the common monitor as selected by the user. This function prevents video data flowing from the High Side Computer to the Low Side Computer via the common monitor.

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 and the source of video data. This function also indicates a successful change of mode to the user.

Appendix C Contents of Distribution Package

Configuration for Evaluation

Hardware

C.1 The hardware component of the TOE subject to evaluation was the Multiple Computer Switch FID004 Version 2.0.

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) **Multiple Computer Switch**: Part Number FID004.

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 cables**: There are four of these cables for connecting the mouse and keyboard of the High and Low Side Computers through the Multiple Computer Switch.

d) **15-pin VGA D-Type male to female cables**: These are two cables for connecting the video outputs of the High and Low Side Computers through the Multiple Computer Switch.

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 Multiple Computer Switch has been received, the following actions should be performed by the administrator:

a) Open the packaging for the Multiple Computer Switch 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

Multiple Computer Switch(es);

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 Multiple Computer Switch case, in accordance with the faxed checklist;

e) Check that the corresponding part number for the Multiple Computer Switch on the checklist is **FID004-2.0** and that this number corresponds to the label on the back of the Multiple Computer Switch. **This is the evaluated version**;

f) Initial against the row with the Mutliple Computer Switch details;

g) Repeat steps c) through f) for all received Multiple Computer Switches 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 Multiple Computer Switch has been installed, the following actions can be performed by an Administrator to verify that the Multiple Computer Switch 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 Mutliple Computer Switch is labelled **FID004-2.0**. **This is the evaluated version**;

c) The version of any Multiple Computer Switch may be confirmed by contacting Vision Abell and supplying the tamper seal serial number and the serial number on the back of the Multiple Computer Switch.