National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Tenix Defence Pty Ltd

Interactive Link Version 5.1 (P/N NIM001)

Report Number: **CCEVS-VR-05-0115**
Dated: **19 August 2005**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Ken Elliott III
The Aerospace Corp.
Columbia, MD

Common Criteria Testing Laboratory

COACT, Inc.
Columbia, Maryland

Table of Contents

1 Executive Summary 1
1.1 Interpretations 2
1.2 Threats to Security 2
2 Identification 4
3 Security Policy 5
4 Assumptions 6
5 Architectural Information 8
6 Documentation 12
7 IT Product Testing 19
7.1 Developer Testing 19
7.2 Evaluation Team Independent Testing 19
7.3 Evaluation Team Penetration Testing 20
8 Evaluated Configuration 20
9 Results of the Evaluation 20
10 Validator Comments/Recommendations 21
11 Annexes 22
12 Security Target 22
13 Glossary 22
14 Bibliography 24

1 Executive Summary

The evaluation of the Tenix Interactive Link (IL) was performed by COACT, Inc. in the United States and was completed on 14 July 2005. This evaluation was augmented by analysis performed by the National Security Agency, as well as two CCEVS Technical Oversight Panels (TOPs). The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0. For evaluation of CC Part 3 components above EAL4 performed by the CCTL, methodology was created by the CCTL and validator and approved by CCEVS. For evaluation of CC Part 3 components above EAL4 performed by NSA, the validator determined that the work performed was commensurate with an EAL5 level of effort.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory, and at the NSA as well, using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1), supplemented with additional methodology. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory and the NSA in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Tenix IL product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. Two Technical Oversight Panels (TOPs) were held as well; one on the design (ADV) of the TOE, and another on the testing (ATE) of the TOE. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the evaluation findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the evaluators in the evaluation technical report are consistent with the evidence produced.

The COACT, Inc. evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4) have been met. In addition, the COACT, Inc. evaluation team concluded that EAL 5 requirements for the ACM components and ALC components have been met. The NSA evaluation team, in addition to work performed by the TOPs, have concluded that the EAL 5 requirements for ADV components, ATE components, and AVA components have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by COACT; the ETR produced by the NSA evaluation teams; and information presented at the TOP activity.

1.1 Interpretations

The following interpretations are incorporated into the evaluation.

National Interpretations

I-0405 – American English Is An Acceptable Refinement, 2000-12-20
I-0407 – Empty Selections Or Assignments, 2002-01-04
I-0427 – Identification of Standards, 2001-06-22

International Interpretations

RI # 3 - Unique identification of configuration items in the configuration list, 2002-02-11
RI # 4 - ACM_SCP..1C requirements unclear, 2001-11-12*
RI # 8 - Augmented and Conformant overlap, 2001-07-31
RI #19 – Assurance Iterations, 2002-02-11
RI # 31 - Obvious vulnerabilities, 2002-10-25
RI #49 – Threats met by the Environment, 2001-02-16
RI #64 – Apparent higher standard for explicitly stated requirements, 2001-02-16
RI # 65 - No component to call out security function management, 2001-07-31
RI # 69 – Informal Security Policy Model, 2001-03-30
RI # 75 - Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1, 2000-10-15
RI #84 – Aspects of objectives in TOE and environment, 2001-02-16
RI #85 – SOF Claims additional to the overall claim, 2002-02-11
RI # 116 - Indistinguishable work units for ADO_DEL, 2001-07-31
RI # 127 – TSS Work unit not at the right place, 2002-10-25
RI # 128 – Coverage of the delivery procedures, 2002-11-15
RI # 133 - Consistency analysis in AVA_MSU.2, 2002-10-25
RI #138 – Iteration and narrowing of scope, 2002-06-05

1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.TRANSFER	A USER or process, e.g. a Trojan horse, on the HIGH SIDE NETWORK that accidentally or deliberately breaches the confidentiality of some HIGH SIDE INFORMATION by transmitting data through the IL-DDD to the LOW SIDE NETWORK.
T.TRANSMIT	A USER or process on the HIGH SIDE NETWORK that accidentally or deliberately breaches the confidentiality of some

HIGH SIDE INFORMATION by transmitting data from a HIGH SIDE WINDOW SERVER through the IL-KBS to the LOW SIDE NETWORK.

T.ACCIDENTAL_ENTRY A USER accidentally types HIGH SIDE data into the keyboard while the IL-KBS is in the LOW MODE and therefore puts the HIGH SIDE data directly onto the LOW SIDE NETWORK.

T.KEYBOARD A rogue keyboard or mouse copies data intended for HIGH SIDE NETWORK, as it is entered, and re-transmits the data to the LOW SIDE NETWORK when the IL-KBS is in the LOW MODE.

T.TAMPER An adversary tampers with the contents of the IL-KBS or IL-DDD during delivery, and/or after installation, albeit prior to operation that may compromise the TOE objectives.

T.LOGIC A USER or process on the LOW SIDE NETWORK transmits data to the TOE that causes a modification to the TSF.

T.FAILURE The Interactive Link products (IL-KBS or IL-DDD) have a hardware failure that allows HIGH SIDE INFORMATION to be transmitted to the LOW SIDE NETWORK and thus makes the INFORMATION available to LOW SIDE USERS.

T.HIGH_DATA HIGH SIDE DATA entered by the user onto the HIGH SIDE through the keyboard and/or mouse may be stored in the KMF data buffer/s, prior to the user initiating a mode change from HIGH to LOW, and later transferred to the LOW SIDE NETWORK.

It is important to note that the protection offered (and the security policy enforced) is one that preserves the confidentiality of the high-side data. No mechanisms concerning the protection of the integrity of the high side data were evaluated.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Where an Evaluation Assurance Level above EAL4 is granted, CCEVS is responsible for ensuring that the additional assurance components are met. For this evaluation, the CCTL and CCEVS determined appropriate methodology for those components of the ACM and ALC families that were different from EAL4 to EAL5, and then monitored the CCTL's compliance to this methodology. For the ADV, ATE, and AVA work units, an NSA evaluation team performed their analysis directly on the requirements (that is, no formal methodology was formulated).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Tenix Interactive Link, version 5.1, Part Number NIM001
Protection Profile	Not applicable.
ST:	*Interactive Link Common Criteria Security Target, Issue*

Item	Identifier
	12.2, 12 August 2005.
Evaluation Technical Report	*Tenix Interactive Link Version 5.1 Evaluation Technical Report,* August 12, 2005.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.1
Conformance Result	CC Part 2 extended, CC Part 3 augmented
Sponsor	Tenix Datagate Inc.
Developer	Tenix Defence Pty Ltd
Common Criteria Testing Lab (CCTL)	COACT, Inc., Columbia, MD
CCEVS Validator	Ken Elliott, The Aerospace Corporation

3 Security Policy

The TOE provides protection of the confidentiality of data on the HIGH SIDE network whose sole connection point to the LOW SIDE network is through the TOE. The TOE provides a unidirectional transmission of electronic signals (information) from a LOW SIDE network to a HIGH SIDE network. All security functions are provided by the Interactive Link (IL) Keyboard Switch (IL-KBS) and IL Data Diode Device (IL-DDD). The information flow control policy can be summarized as:

Non-Interference TOE Security Policy (TSP)

> Non-interference can be stated informally a number of ways. For the Interactive Link application, it is suggested that the best statement of the theory is as follows. A system is said to be non-interfering if the (LOW) observed outputs of the system are completely determined by the LOW inputs. That is if we have two machines where the LOW inputs are the same, the observed outputs will be the same regardless of any HIGH inputs that may have occurred to one of the machines.

This is the common security policy for all functions of the TOE that cross the secure boundary between the HIGH and LOW SIDE, namely the IL-DDD and the IL-KBS.

4 Assumptions

The Interactive Link provides a connection between two networks of different security levels; HIGH SIDE NETWORK and the LOW SIDE NETWORK. Note that all HIGH SIDE USERS must be cleared to use the LOW SIDE NETWORK. The assumptions made about the intended environment are:

A.PERSONNEL — The Interactive Link shall be installed, administered and used by authorized personnel who possess the necessary privileges to access the HIGH SIDE INFORMATION.

A.PHYSICAL — The intended environment will be capable of storing and operating the devices of the Interactive Link TOE, comprising the IL-KBS and the ILDDD, in accordance with the requirements of the HIGH SIDE NETWORK. Information systems have different requirements for the storage of computer equipment used for processing information of different security levels. There may also be a requirement for protecting critical system resources within secured rooms. The IL-DDD is critical to all the USERS of the Interactive Link and requires no administrator control after it has been installed. It is the SYSTEM MANAGEMENT STAFF responsibility to protect it from accidental or deliberate tampering causing its functionality to be bypassed. The IL-KBS has no long term data storage devices from which secure INFORMATION can be obtained, and is intended to be kept on the USER's desk top, within the same environment as the HIGH SIDE NETWORK.

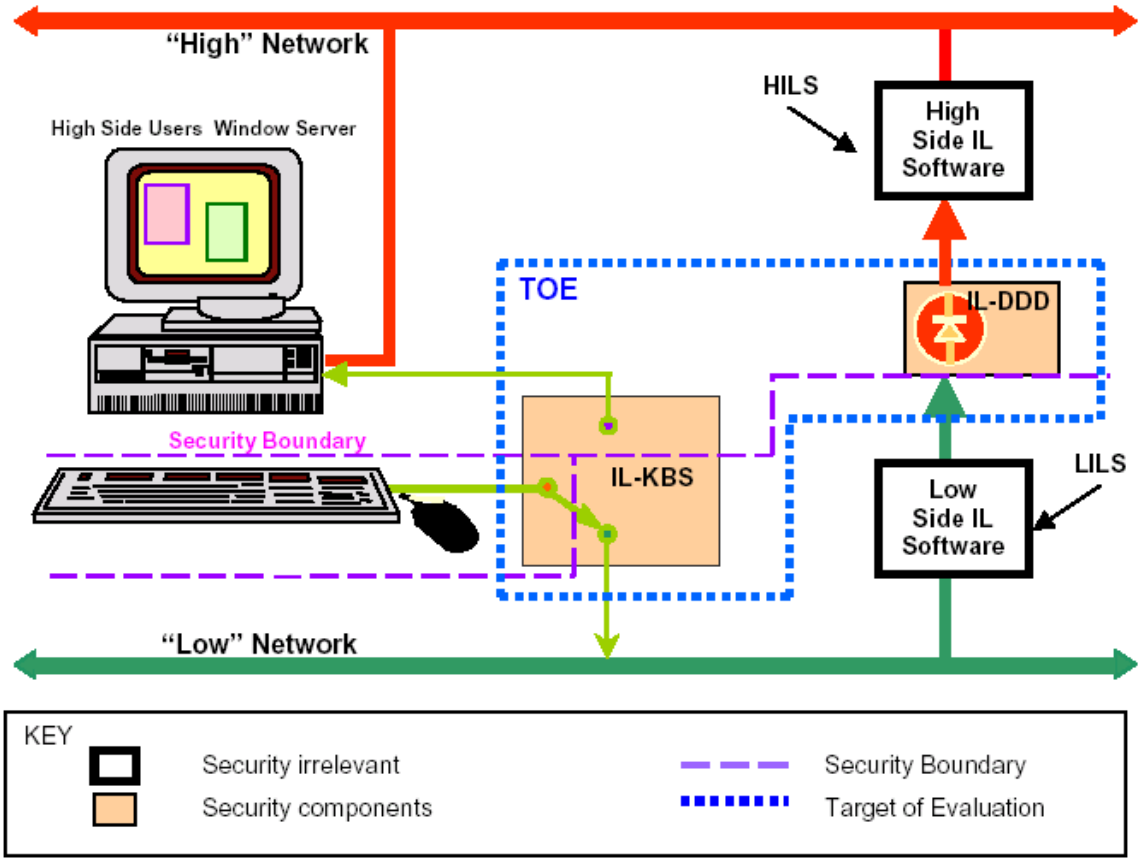
A.EMISSION — It is intended that the devices operate in an environment where physical (or some other) security measures prevent any TEMPEST attack. This could be achieved by ensuring that the security boundary is outside the Interactive Link Equipment Radiation TEMPEST Zone (ERTZ). The Interactive Link products operate at the edge of the secure boundary where the LOW SIDE NETWORK meets the HIGH SIDE NETWORK. Care should be taken to determine the relationship of the Interactive Link products ERTZ to their secure boundaries and to keep the ERTZ within them. This will ensure that any attempt to mount a TEMPEST attack would not compromise the security of the INFORMATION system.

A.INSTALLATION — The SYSTEM MANAGEMENT STAFF will install the trusted devices of the Interactive Link correctly and in accordance with the Administration Documentation. The installation of the Interactive

	Link system is to be accredited by the appropriate SECURITY AUTHORITY.
A.PROCUREMENT	Equipment hardware and software procurement policies are to be followed to minimize the risk of installing malicious hardware and software.
A.TRAINING	All staff who have access to a secure INFORMATION systems 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.
A.USER	The USER while in HIGH MODE will stop typing HIGH SIDE data before selecting the button on the front of the IL-KBS to change it to LOW MODE. The user shall not type HIGH SIDE data until the IL-KBS has been changed back to HIGH MODE. Thus USER will not place HIGH SIDE data directly onto the LOW SIDE NETWORK.
A.NETWORK	Interactive Link products are the only method of interconnecting the LOW and HIGH SIDE NETWORKS. This prevents a threat agent from circumventing the security being provided by the Interactive Link through an untrusted product/path.
A.NO_EVIL	Authorized users of the TOE are non-hostile and follow all usage guidance to ensure that the Interactive Link is operated in a secure manner.

5 Architectural Information

The Target of Evaluation (TOE) of the Interactive Link solution consists of hardware and firmware components. These hardware and firmware components satisfy the security objectives of the TOE, and are the Interactive Link-Keyboard Switch (IL-KBS) and the Interactive Link-Data Diode Device (IL-DDD), pictured below. These are two physically separate hardware "boxes"; the IL-KBS providing a means to switch the connected keyboard and mouse between the low-side network and high-side network (similar to a KVM switch), while the IL-DDD provides a one-way flow of data from the low-side network to the high-side network.

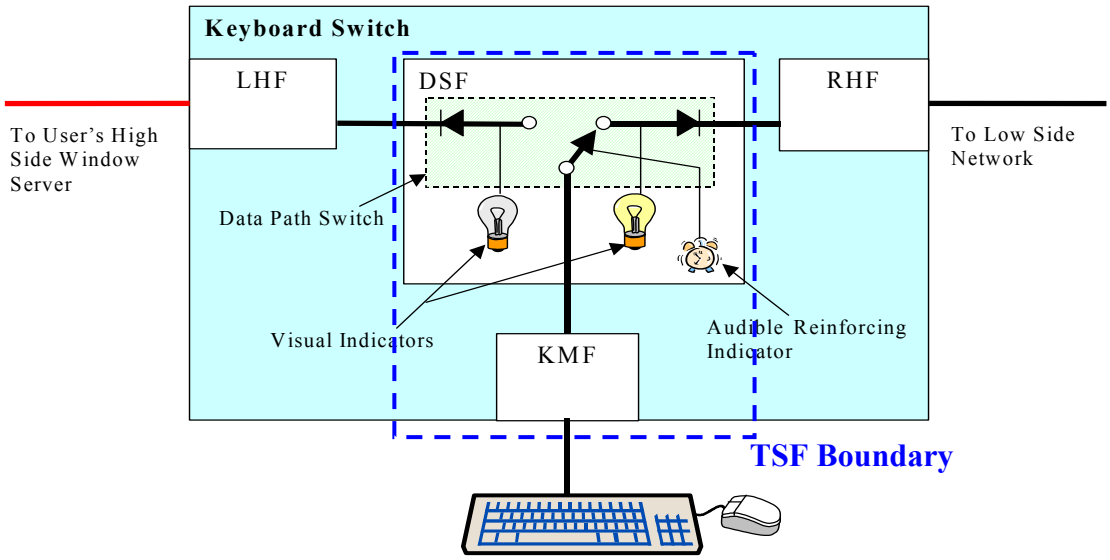


A number of additional components are pictured above; while not part of the TOE, these additional components are necessary in order for a user to be able to manipulate data at both the high and low levels on the pictured workstation. These components are described in the IT Environment section below.

IL-KBS

The IL-KBS contains both firmware and hardware, and consists of the following functional blocks as shown in the diagram below.

- Data Switch Function (DSF);
- Keyboard Mouse Function (KMF);
- Local Host Function (LHF); and
- Remote Host Function (RHF).



As depicted above, the TSF boundary (for the IL-KBS) includes only two of the 4 components of the IL-KBS, even though all four components are implemented on the same integrated hardware unit.

The architecture pictured above provides the following features:

• Keyboard buffers are protected from clandestine listeners on either side of the switch;
• Visual indication of the connected network.
• While in LOW MODE a session is conducted on a remote server on the LOW SIDE NETWORK.

The IL-KBS enables the USER to switch the keyboard and mouse (COMMON PERIPHERALS) to either the HIGH SIDE desktop or the LOW SIDE NETWORK. Keyboard and mouse data entered in the IL-KBS is processed by the Keyboard Mouse Function (KMF) before passing to the Data Switch Function (DSF). The DSF provides the switching functionality and passes the data onto either the Local Host Function (LHF), which interfaces to the USERS HIGH SIDE WINDOW SERVER, or the Remote Host Function (RHF) that interfaces to the LOW SIDE

NETWORK. Note that communications with the LOW SIDE NETWORK is performed by the RHF, which is outside of the TSF.

IL-DDD

The IL-DDD is implemented solely in hardware. The IL-DDD provides a unidirectional data path from the LOW SIDE NETWORK to the HIGH SIDE NETWORK. Features include:

- Data transfer over the diode is sent without acknowledgment;
- Multiple workstations or PCs can share a single Data Diode.

The Interactive Link provides a one-way data flow from the LOW SIDE NETWORK to the HIGH SIDE NETWORK via the IL-DDD. The Interactive Link software (which is not part of the TOE, but runs in the IT Environment as explained below) provides the method for the keyboard and mouse data to interact with a LOW SIDE window session. The output is then packaged for transmission to the HIGH SIDE where it is forwarded to the USER'S HIGH SIDE WINDOW SERVER. The IL-DDD provides the physical media for the Interactive Link operation and all the security functionality. USERS can interact with applications and INFORMATION on either the HIGH SIDE NETWORK or the LOW SIDE NETWORK by having the keyboard and mouse data switched to the appropriate output port of the IL-KBS. Access to either the LOW or HIGH SIDE NETWORK is controlled by the USER pressing either the HIGH or LOW buttons on the front panel of the IL-KBS, thus changing the MODE of the IL-KBS.

The USER can have multiple HIGH or LOW windows displayed on the HIGH SIDE WINDOW SERVER's screen, generated from applications running on both the HIGH and LOW SIDE NETWORKS; the Interactive Link provides the connectivity to link the keyboard/mouse to the high side or low side, and to transmit data from the low side to the high side. In the evaluated configuration, the Interactive Link products must be the only method of connecting the LOW or HIGH SIDE NETWORKS. This prevents a threat agent from circumventing the security provided by the IL-KBS or IL-DDD through an untrusted product or path.

When the USER selects the HIGH MODE, the keyboard and mouse are connected to the workstation or PC so that HIGH SIDE data is passed to the HIGH SIDE WINDOW SERVER allowing interaction with the HIGH SIDE. When the LOW MODE is selected, the keyboard and mouse are connected through the LOW SIDE NETWORK to an application server that is outside of the TOE. The application output is passed to and displayed on the user's HIGH SIDE WINDOW SERVER via the IL-DDD. The IL-KBS provides visual indication as to which network is currently accessed.

IT Environment

The IT environment provides support for the TOE, allowing the TOE to operate with full functionality. The IT environment includes the HIGH and LOW SIDE Interactive Link servers,

IL software and a keyboard and mouse. The software resident on the LILS gives the server the ability to interpret the keyboard and mouse information from the IL-KBS and conduct an interactive windows session on the LOW SIDE. The LOW SIDE software then pipes the display data to the HIGH SIDE via the IL-DDD. The software resident on the HIGH SIDE server then maps the session data to the appropriate USER'S HIGH SIDE WINDOW SERVER to be displayed.

The following components are required for the IT environment and are necessary to deploy the complete Interactive Link architecture; it should be noted, however, that these dependencies are in almost all instances for functional purposes. The only dependency that has an impact on the security functionality is the keyboard; implications of this dependency are detailed in section 10, *Validator Comments/Recommendations*.

• The HIGH SIDE Interactive Link Server (HILS) consists of hardware, a commercial operating system and purpose built software, and contains no security functions.
• The LOW SIDE Interactive Link Server (LILS) consists of hardware, a commercial operating system and purpose built software which contains no security functions.
• The IL Software is purpose built software, has different aspects resident on both the HILS and the LILS, and contains no security functions.
• The HIGH SIDE USER'S WINDOW SERVER, consists of hardware, a commercial operating system and COTS software, and it contains no security functions.
• The Keyboard and Mouse utilises a standard 104-key keyboard, 3-button wheel mouse or a Sun™ standard keyboard and mouse combination.

The IL-DDD is installed between the HIGH and LOW SIDE NETWORKs and is located with the HILS, in the HIGH SIDE NETWORK space. The HILS receives LOW SIDE INFORMATION transferred across the IL-DDD from the LILS. The HILS distributes INFORMATION to the appropriate HIGH SIDE USER'S WINDOW SERVER. The LILS runs the LOW SIDE window session, though applications can be executed on any server on the LOW SIDE NETWORK. The LILS then packages up the display INFORMATION so that it can be transferred across the unidirectional IL-DDD.

The existing keyboard and mouse will be connected through the IL-KBS to the HIGH SIDE USER'S WINDOW SERVER. There will also be a connection between the IL-KBS and the LOW SIDE NETWORK. The connections with the IL-KBS are bi-directional to cater for the hand shaking required by the keyboard and mouse, the USER'S WINDOW SERVER and the LOW SIDE NETWORK protocol, TCP/IP.

6 Documentation

The following documentation was supplied to support the evaluation of the TOE.

Document	Version
IL SUPPORTING DOCUMENTATION (96162D00001001DL.xls)	Issue 1
IL PRODUCTS (96162D00001001IL.xls)	Issue 5
UNIT TRANSPORTABLE (96162D00002001PL.XLS)	Issue 1
INTERACTIVE LINK SYSTEM (96162D00003001CL.xls)	Issue 4
KEYBOARD SWITCH 10BASE-T SHIPPABLE (US) (96162D01001001-003CL.xls)	Issue 4
KEYBOARD SWITCH (96162D01001001DL.xls)	Issue 3
KBS ACCESSORY PACK (US) (96162D01100001-001PL.xls)	Issue 1
KBS (10BASE-T) SHIPPABLE (US) (96162D01200001-006PL.xls)	Issue 2
KBS ASSEMBLY (10BASE-T) (96162D01305001CL.xls)	Issue 3
KBS ASSEMBLY (10BASE-T) (96162d01305001PL.xls)	Issue 8
KEYBOARD SWITCH 10BASE-T CIRCUIT CARD ASSEMBLY (96162D01310001-001CL.xls)	Issue 1
KEYBOARD SWITCH 10BASE-T CIRCUIT CARD ASSEMBLY (96162D01310001-001PL.xls)	Issue 1
KEYBOARD SWITCH 10BASE-T PROGRAMMED CCA (96162D01311001-001CL.xls)	Issue 1
KEYBOARD SWITCH 10BASE-T PROGRAMMED CCA (96162D01311001-001PL.xls)	Issue 1
FRONT PANEL CIRCUIT CARD ASSEMBLY (96162D01320001CL.xls)	Issue 1
FRONT PANEL CIRCUIT CARD ASSEMBLY (96162d01320001PL.xls)	Issue 4
INTERACTIVE LINK APPROVED SOURCES LISTING (96162d01990200.xls)	Issue 6
DATA DIODE DEVICE SHIPPABLE (US) (96162D02400001-001CL.xls)	Issue 4
DATA DIODE DEVICE SHIPPABLE (US) (96162D02400001-001PL.xls)	Issue 5
DATA DIODE DEVICE (96162D02400001DL.xls)	Issue 3
DATA DIODE DEVICE ACCESSORY PACK (US) (96162D02410001-001PL.xls)	Issue 1
DATA DIODE DEVICE ASSEMBLY (96162D02430001CL.xls)	Issue 3
DATA DIODE DEVICE ASSEMBLY (96162d02430001PL.xls)	Issue 7
DATA DIODE DEVICE CIRCUIT CARD ASSEMBLY (96162D02431001CL.xls)	Issue 2

Document	Version
DATA DIODE DEVICE CIRCUIT CARD ASSEMBLY (96162d02431001PL.xls)	Issue 4
ADMINISTRATOR PACK (96162D04001001CL.xls)	Issue 3
ADMINISTRATOR PACK (96162d04001001PL.xls)	Issue 4
HIERARCHY.doc	None
SUPPORT SYSTEMS PROCEDURE DOCUMENT AND DATA CONTROL (msp0702.doc)	Issue 3.1
Configuration Management Documentation (B217P00001001.pdf)	Issue 1.0
KBS Assembly Procedure (96162k01990101.doc)	Issue 1
DDD Assembly Procedure (96162K01990102.doc)	Issue 1
WORK INSTRUCTION FOR CLEARCASE CONFIGURATION MANAGEMENT (infosec_wi_050201.doc)	Issue 3.0
WORK INSTRUCTION FOR IMPLEMENTING A RELEASE BASELINE (infosec_wi_050202.doc)	Issue 2.0
Janus Phase 1 Version Description Document (Janus Ph1 VDD.doc)	Issue 1.0
DDD_2.1.4_CAD.TXT	None
DDD_2.1.4_DOCS.TXT	None
IL_RELEASE_5.0.1_CAD.TXT	None
IL_RELEASE_5.0.1_DOCS.TXT	None
IL_RELEASE_5.0.1_SOURCE.TXT	None
KBS_10BASET_2.1.0_CAD.TXT	None
KBS_10BASET_2.1.0_DOCS1.TXT	None
KBS_10BASET_2.1.0_SOURCE.TXT	None
KBS_MAN_6.0.1_DOCS.txt	None
KBS_MAN_6.0.1_SOURCE.txt	None
SUPPORT_EQUIP_1.1.0_DOCS.txt	None
tool_config.txt	None
Infosec Documentation.xls	None
Infosec ECO Register.xls	None
Infosec ECP Register.xls	None
Software.xls	None
Software_COTS.xls	None
Software_ESD.xls	None
PROJECT MANAGEMENT PROCEDURES DEVELOPMENT DOCUMENTATION SYSTEM (DDS) STANDARD (msi040101.doc)	Issue 1
PROJECT MANAGEMENT PROCEDURES PROJECT MANAGEMENT (msp0401.doc)	Issue 2
ENGINEERING PROCEDURES CONFIGURATION CONTROL (msp0502.doc)	Issue 2.1
ENGINEERING PROCEDURES CONTROL OF THE DEVELOPMENT ENVIRONMENT (msp0505.doc)	Issue 2

Document	Version
SUPPORT SYSTEMS PROCEDURE DOCUMENT AND DATA CONTROL (msp0702.doc)	Issue 3.1
Configuration Management Plan (CMP_v4.3_B214.P01.000.003.doc)	Issue 4.3
ECP Template (sd001.doc)	Issue 1
ECO Template (sd002.doc)	Issue 1
Corrective Action Request Template (sd013.doc)	Issue 1
Nonconformance/Trouble Report (sd009.doc)	Issue 1
Contract Change Proposal (sd199.doc)	Issue 1
Request for Deviation/Waiver (sd080.doc)	Issue 1
B217D001002 Configuartion Control Identification Register (CCI_register.doc)	Issue 2.0
ECP226 Evidence (ECP226.doc)	N/A
ECP226 Evidence (ECP226trail.doc)	N/A
WORK INSTRUCTION FOR DELIVERY PROCEDURES FOR INTERACTIVE LINK COMPONENTS (infosec_wi_060201.doc)	Issue 2.0
Tenix Datagate US Work Instruction For Purchase Order Validation (Purchase_Order_Validation_TDUS-WI-030301_v1.1.doc)	Issue 1.1
Tenix Datagate US Work Instruction For Quotations (Quotations-TDUSWI-030302.doc)	Issue 1.0
Tenix Datagate Work Instruction For Sales Order Processing (Sales_Order_Processing_TDC-WI-030301.doc)	Issue 1.0
Delivery and Operation Procedures (B217P00001003.pdf)	Issue 1.0
Functional Specification (B217P00002002_v7.doc)	Issue 7
High Level Design (B217P00002003_v8`.doc)	Issue 8
Engineering Specification for the Type 5 Keyboard and Mouse Interface Rev A IBM Personal System/2 Mouse Technical Reference	Second Edition
IBM Personal System/2 Hardware Interface Technical Reference - Common Interfaces	First Edition
Data Diode Device Implementation (B217P00002008.pdf)	Issue 3.0
Drawing 96162D01310002 Keyboard Switch Schematic Diagram 22 sheets (96162D01310002_9.pdf)	Issue 9
Drawing 96162D01310001 Keyboard Switch Circuit Card Assembly 1 sheet (96162D01310001_6.pdf)	Issue 6
Drawing 96162D01310020 Keyboard Switch Printed Board 8 sheets (96162D01310020_7.pdf)	Issue 7
Drawing 96162D01320001 Front Panel Circuit Card Assembly 1 sheet (96162D01320001_r3.pdf)	Issue 3
Drawing 96162D01320002 Front Panel Schematic Diagram 1 sheet (96162D01320002_r2.pdf)	Issue 2
Drawing 96162D01320020 Front Panel Printed Board 6 sheets (96162D01320020_r3.pdf)	Issue 3

Document	Version
Drawing 96162D02431001 Data Diode Device Circuit Card Assembly 1 sheet (96162D02431001_2 .pdf)	Issue 2
Drawing 96162D02431002 Data Diode Device Schematic Diagram 1 sheet (96162D02431002_2.pdf)	Issue 2
Drawing 96162D02431020 Data Diode Device Printed Board 8 sheets (96162D02431020_2 .pdf)	Issue 2
Interactive Link Implementation (B217P00002006_V6.0.doc)	Issue 6.0
hfbr11xx.pdf	None
hfbr-1115_2115.pdf	None
hp.eps	None
motorola_mc10h188_rev5.pdf	None
pin_conversionrev6.pdf	None
schs123.pdf	None
schs182.pdf	None
scls085b.pdf	None
scls088b.pdf	None
scls100b.pdf	None
scls116c.pdf	None
scls181b.pdf	None
scls305a.pdf	None
Interactive Link Semiformal Low-level Design (B217P00002004_v4.doc)	Issue 4.0
Data Diode Device Semiformal Low-level Design (B217P00002009.doc)	Issue 3.0
Correspondence Demonstration (B217P00002007.v6.doc)	Issue 6
Security Policy Model (B217P00002001.doc)	Issue 6.0
INTERACTIVE LINK FORMAL POLICY AND ARCHITECTURE (9125P01000014.pdf)	Version 3.0
Interactive Link Guidance Documentation (B217P00003001.pdf)	Issue 1.0
IL-DDD INSTALLATION AND ADMINISTRATION GUIDE (96162H05001001_v17.pdf)	Issue 17
IL-KBS WORKSTATION INSTALLATION AND USER GUIDE (96162H01300001_V15.pdf)	Issue 15
Interactive Link Life Cycle Support Documentation (B217P00001004.pdf)	Issue 2.0
PROJECT MANAGEMENT PROCEDURES DEVELOPMENT DOCUMENTATION SYSTEM (DDS) STANDARD (msi040101.doc)	Issue 1
WORK INSTRUCTION FOR PROTEL CAD SYSTEM (msi050502.doc)	Issue 2.0
WORK INSTRUCTION FOR PRINTED BOARD DESIGN USING COMPUTER AIDED DESIGN (CAD) (msi050503.doc)	Issue 1

Document	Version
QUALITY SYSTEM PROCEDURES REVIEW AND AUDIT (msp0102.doc)	Issue 3.2
PROJECT MANAGEMENT PROCEDURES PROJECT MANAGEMENT (msp0401.doc)	Issue 2.0
ENGINEERING PROCEDURES CONTROL OF CUSTOMER SUPPLIED PRODUCT (msp0501.doc)	Issue 2.1
ENGINEERING PROCEDURES CONFIGURATION CONTROL (msp0502.doc)	Issue 2.1
ENGINEERING PROCEDURES INSPECTION AND TESTING (msp0503.doc)	Issue 2.1
ENGINEERING PROCEDURES CONTROL OF THE DEVELOPMENT ENVIRONMENT (msp0505.doc)	Issue 2
PRODUCTION PROCEDURES MANUFACTURE AND PROCESS CONTROL (msp0601.doc)	Issue 3
PRODUCTION PROCEDURES RECEIPT, HANDLING AND DELIVERY (msp0602.doc)	Issue 2.2
PRODUCTION PROCEDURES CONTROL OF INSPECTION, MEASURING AND TEST EQUIPMENT (msp0603.doc)	Issue 2
SUPPORT SYSTEMS PROCEDURE PURCHASING SUPPLIES AND SELECTING AND CONTROLLING SUBCONTRACTORS (msp0701.doc)	Issue 3
SUPPORT SYSTEMS PROCEDURE DOCUMENT AND DATA CONTROL (msp0702.doc)	Issue 4.0
SUPPORT SYSTEMS PROCEDURES CONTROLLING AND CORRECTING DEFICIENCIES (msp0703.doc)	Issue 2
Project Management Plan (PMP_v1.0_B214.P01.000.002.doc)	Issue 1.0
Project Quality Plan (QMP_v2.0_B214.P01.000.00_v2draft.doc)	Issue 2.0
WORK INSTRUCTION FOR DRAWING OFFICE PRACTICES (sda040105.doc)	Issue 1
WORK INSTRUCTION FOR SECURITY PRACTICES AND PROCEDURES (SDAWI020501v02.doc)	Issue 2.0
WORK INSTRUCTION FOR INFORMATION SYSTEMS SECURITY PRACTICES AND PROCEDURES (SDAWI020504_v2.1.doc)	Issue 2.1
Interactive Link Programming Languages and Compilers (il-languagescompilers.doc)	Issue 1
Functional Tester Description (96162E01810001.doc)	Issue 2
KBS/MCS Functional Test Procedure (96162k01000045.doc)	Issue 1
KBS/MCS Programming & Security Function Test Procedure (96162k01990100.doc)	Issue 1
Janus Phase 2B – Version Description Document (Janus P2b Version Description.doc)	Issue 1.3

Document	Version
IL-KBS / IL-MCS Bed-Of-Nails Description (kbs_mcs_bon_description.doc)	Issue 0.1/010
System Engineering Management Plan (SEMP.doc)	Issue 1.0
Software Development Plan (SW_development_plan.doc)	Issue 1.1
Interactive Link Version 1 Test and Evaluation Master Plan (V1_test_eval_master_plan.doc)	Issue 2.1
Contract/Technical Progress Report for June 2000 (cprJune2000_issue1.doc)	Jun-00
DDTS (ddts.doc)	None
Infosec Master Schedule (infomstr_26Jan01.pdf)	1/26/2001
Release Note (sd038.doc)	Issue 1
Software Inspection Record (sd109.doc)	Issue 1
Document Review Record (sd204.doc)	Issue 2
Borland C++ QuickTour	Version 4.5
Borland C++ DOS Reference	Version 4.5
Borland C++ Library Reference	Version 4.5
Borland C++ User's Guide	Version 4.5
Borland C++ Programmer's Guide	Version 4.5
Borland C++ Class Library Guide	Version 4.5
Borland Turbo Debugger User's Guide	Version 4.5
Borland Turbo Profiler User's Guide	Version 4.5
Borland ObjectWindows Tutorial	Version 2.5
Borland ObjectWindows Reference Guide	Version 2.5
Borland ObjectWindows Programmer's Guide	Version 2.5
Interactive Link Common Criteria Security Target	Issue 12.2
Tests (B217P00004001_v7.doc)	Issue 7
Tests (B217P00004001_v7.doc)	Issue 7
Interactive Link CC Evaluation Master Test Plan (B217P00004002_V6.0.doc)	Issue 6
Interactive Link CC Evaluation Test Bed Setup and Demonstration (B217P00004014_v2.doc)	Issue 2.0
TR001 Test Procedure (B217P00004003.v4.doc)	Issue 4
TR002 Test Procedure (B217P00004004.V4.doc)	Issue 4
TR003 Test Procedure (B217P00004005.V4.doc)	Issue 4
TR004 Test Procedure (B217P00004006.V4.doc)	Issue 4
TR005 Test Procedure (B217P00004007.V4.doc)	Issue 4
TR006 Test Procedure (B217P00004008.v4.doc)	Issue 4
TR007 Test Procedure (B217P00004009.v4.doc)	Issue 4
TR008 Test Procedure (B217P00004010_V3.0.doc)	Issue 3
TR009 Test Procedure (B217P00004011_V3.0.doc)	Issue 3

Document	Version
TR010 Test Procedure (B217P00004016_V3.0.doc)	Issue 3
TR011 Test Procedure (B217P00004012_V4.0.doc)	Issue 4
TR013 Test Procedure (B217P00004013_V5.0.doc)	Issue 5
TR014 Test Procedure (B217P00004015_V3.0.doc)	Issue 3
TR015 Test Procedure (B217P00004032_V2.0.doc)	Issue 2
TR016 Test Procedure (B217P00004033_V3.0.doc)	Issue 3
TR017 Test Procedure (B217P00004034_V2.0.doc)	Issue 2
Tests (B217P00004001_v7.doc)	Issue 7
TR001 Test Result (B217P00004036_v1.pdf)	Issue 1
TR002 Test Result (B217P00004037_v1.pdf)	Issue 1
TR003 Test Result (B217P00004038_v1.pdf)	Issue 1
TR004 Test Result (B217P00004039_v1.pdf)	Issue 1
TR005 Test Result (B217P00004040_v1.pdf)	Issue 1
TR006 Test Result (B217P00004041_v1.pdf)	Issue 1
TR007 Test Result (B217P00004042_v1.pdf)	Issue 1
TR008 Test Result (B217P00004043_v1.pdf)	Issue 1
TR009 Test Result (B217P00004025_v1.pdf)	Issue 1
TR010 Test Result (B217P00004045_v1.pdf)	Issue 1
TR011 Test Result (B217P00004046_v1.pdf)	Issue 1
TR013 Test Result (B217P00004047_v1.pdf)	Issue 1
TR014 Test Result (B217P00004048_v1.pdf)	Issue 1
TR015 Test Result (B217P00004049_v1.pdf)	Issue 1
TR016 Test Result (B217P00004050_v1.pdf)	Issue 1
TR017 Test Result (B217P00004051_v1.pdf)	Issue 1
Binding and Covert Channel Analysis (B217P00005001_v2.0.doc)	Issue 2
Evaluation of Misuse for Interactive Link (B217P00005005_v3.0.pdf)	Issue 3.0
Evaluation of Misuse for Data Diode Device (B217P00005002_v2.0.pdf)	Issue 2.0
Vulnerability Analysis – Highly Resistive for the Data Diode Device (B217P00005004_V2.0.pdf)	Issue 2
Vulnerability Analysis – Highly Resistive for the Interactive Link (B217P00005006_V4.0.pdf)	Issue 4

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The vendor ran the documented test procedures before the evaluation team's Independent Testing Activity began. The vendor provided a complete set of test results for analysis.

Both the CCTL and NSA evaluators analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected, and determined that the developer's actual test results matched the vendor's expected results. The CCTL analysis covered interfaces and depth to the subsystem level, while the NSA analysis looked at testing to the low-level design.

Developer testing consists of both informal and formal testing. Informal testing is performed by engineers at various points in the development process, while formal testing is documented in the procedures examined by the evaluators. Since the devices are implemented in hardware and firmware, testing consists not only of testing at the external interfaces of the physical device, but also at test points utilizing a device called a "Bed of Nails" (BON). This device allowed testing internal to the TSF, as well as directly at the TSF boundary.

There were four configurations tested. The IL-DDD was tested when connected between two workstations, one simulating the high side, one simulating the low side. The IL-KBS was tested both on the BON device, as wells as in a "stand-alone mode" (that is, the devices' inputs and outputs were stimulated by various test equipment). Finally, the entire IL was tested in a "complete" configuration, as it would be used in operation.

7.2 Evaluation Team Independent Testing

The CCTL ran all of the developer tests. Since the BON is specialized test equipment not available at the CCTL facility, the evaluators traveled to the developer's facility to run these tests. Other independent testing was conducted at the CCTL facility. All four test configurations were utilized, since the coverage of the developer tests was complete.

The CCTL also performed additional functional testing. These tests were formulated by analyzing the functional testing performed by the developer, and noting areas where the testing was sufficient to satisfy the ATE requirements, but where the interface or function was not completely tested (for instance, more complete boundary condition testing). These additional tests did not result in any unexpected results.

7.3 Evaluation Team Penetration Testing

Penetration testing on the TOE was performed both by CCTL and NSA evaluators. Testing performed by the CCTL demonstrated penetration resistance commensurate with AVA_VLA.2, while that done by the NSA demonstrated penetration resistance commensurate with AVA_VLA.3. Testing was based on examination of the high- and low-level design, including schematics and firmware listings. This analysis included an examination of the interfaces between the DSF and both the RHF and LHF, as well as an examination of the interface presented by the KMF.

Penetration testing also was targeted at ADO claims on the tamper resistant seals incorporated into the TOE. Proprietary test reports were generated for both the CCTL and NSA activities.

8 Evaluated Configuration

The evaluated configuration consists of the Interactive Link (IL-KBS and IL-DDD) designated as Tenix Interactive Link, version 5.1, Part Number NIM001. The devices require no configuration, other than attaching the appropriate connections. Note that the TOE must be the only connection between the low network and the high network. While mis-configuration of the software in the IT Environment (as described above) may result in an inability to perform useful work, it will not effect the enforcement of the confidentiality of high-side data and thus has no security impact on the evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0. For evaluation of CC Part 3 components above EAL4 performed by the CCTL, methodology was created by the CCTL and validator and approved by CCEVS. For evaluation of CC Part 3 components above EAL4 performed by NSA, the validator determined that the work performed was commensurate with an EAL5 level of effort, and adequately addressed the EAL5 requirements.

Both Evaluation Teams assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Teams advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the

assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

In addition to the activities of the Evaluation Teams, CCEVS performed two Technical Oversight Panel activities on the product. The first panel addressed the ADV class, focusing on the accuracy of the CCTL's analysis of that evidence. While some discrepancies were found, the evidence was found to be largely satisfactory and was subsequently brought into compliance with the requirements. The second panel addressed the ATE class, with some amount of focus on the AVA_VLA activities. This panel found no major deficiencies with the test plan, developer's test methodology and results, nor with the proposed penetration testing.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

10 Validator Comments/Recommendations

In addition to the information presented in other sections of this document, the validator has the following comments:

Evaluated Configuration: The TOE consists only of the two physical devices comprising the Interactive Link: the Keyboard Switch and the Data Diode Device. While these devices perform their security functions in accordance with the ST, it is important for users to understand that other, unevaluated, software and hardware is necessary to provide the functionality described in most product literature (e.g., the ability to cut from a low-side document and paste to a high-side document). The use and configuration of this supporting software and hardware will have to be assessed in the user's environment.

Provided Security Functionality: It is also important for users to understand that the scope of the evaluation focused on the TOE's ability to protect high-side data from being disclosed to low-side entities. There was no evaluation of the capability for low-side entities to corrupt high-side data, and similarly no evaluation of the capability for low-side entities to deny service to high-side entities.

IT Environment Requirements in the ST: The keyboard is not part of the TOE and was not evaluated. There is a requirement that the keyboard empty its buffers within a defined time period; if it does not do this, then there is a potential for high side data being typed into the keyboard to appear on the low side. In the evaluation, several keyboards were tested and demonstrated that they emptied their buffers well within the required time.

However, the assurance that the keyboard performs in this fashion is limited to a "black box" testing methodology. Users must assess the risk of using a particular keyboard in their configuration, taking into account other factors such as physical protection of the devices and potential amount and consequences of any high side data "overflow".

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Interactive Link Common Criteria Security Target, Issue 12.2,* 12 August 2005.

The document identifies the security functional requirements (SFRs) necessary to implement Information Flow Protection and TOE Self Protection security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 5.

13 Glossary

The following definitions are used throughout this document:

Application Server refers to a server computer, which executes application software that interacts with a USER.

Common Peripherals refers to the keyboard and mouse that are connected to a computer, but normally mounted outside of the computer enclosure.

Data Diode Device refers to a device that allows the flow of data in one direction only.

Hardware refers to the physical equipment used to process programs.

High Mode indicates that the PERIPHERAL DATA is directed to the users HIGH SIDE WINDOW SERVER.

High side is a descriptor used to refer to items associated with the HIGH SIDE NETWORK.

High side Network refers to the network including computer of which the USER'S local WINDOW SERVER is part. It has a security level greater that the LOW SIDE NETWORK.

Information the INFORMATION is an object, it is considered in two forms: LOW SIDE INFORMATION and HIGH SIDE INFORMATION.

Infosec refers to Information System Security.

Interactive Link is the collection of products that provides the functionality of an interactive link between the HIGH SIDE NETWORK and the LOW SIDE NETWORK with out compromising the confidentiality of the INFORMATION on the HIGH SIDE. The Interactive Link consists of two prime components that provide the security, the KEYBOARD SWITCH and a DATA DIODE DEVICE.

Interface Ports are associated with the IL-DDD, there are two forms of the subject INTERFACE PORTS the INPUT PORT and OUTPUT PORT.

Keyboard Switch refers to a device that allows the keyboard and mouse to connect to the USER'S local WINDOW SERVER on the HIGH SIDE NETWORK or an APPLICATION SERVER on the ***LOW SIDE NETWORK***. The KEYBOARD SWITCH has two buttons and two illuminators referred to in this document as HIGH and LOW. By pressing either button the keyboard and mouse will be connected to the appropriate network.

Low Mode indicates that the PERIPHERAL DATA is directed to the LOW SIDE NETWORK.

Low side is a descriptor used to refer to items associated with the LOW SIDE NETWORK.

Low side Network refers to the network that has a security level lower than the HIGH SIDE NETWORK.

Mode is the state of the IL-KBS, which can be in either LOW MODE or HIGH MODE. In LOW MODE the PERIPHERAL DATA is directed to the LOW SIDE NETWORK. While in HIGH MODE, the PERIPHERAL DATA is directed to the USERS WINDOW SERVER.

Non-Interference is the formal security policy of the Interactive Link. The policy was defined in the papers written by Goguen and Meseguer in 1982 and 1984.

Peripheral Data refers to Keyboard and Mouse output.

Peripheral Port Group refers to Keyboard and Mouse peripheral interface port and is used to define the Information Flow Functionality exercised by the IL-KBS. There are three distinct port groups: ***Common*** – Keyboard and Mouse data input to the IL-KBS and the KMF; ***Low Side*** – Keyboard and Mouse data output from the IL-KBS via the RHF to the LOW SIDE NETWORK; ***High Side*** – Keyboard and Mouse data output from the IL-KBS via the LHF to the HIGH SIDE NETWORK.

Security Authority refers to an independent third party that has been assigned the responsibility to mandate secure usage of the HIGH SIDE classified INFORMATION by the

ultimate owner of the INFORMATION.

Software refers to the programs and associated data that can be dynamically written and modified.

System Management Staff is responsible for the installation and maintenance of the Interactive Link devices and software.

TEMPEST refers to electromagnetic emanations that can be related to the INFORMATION being processed by an INFORMATION system.

Target of Evaluation (TOE) refers to an information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Unidirectional Network Bridge refers to the software that supports data to flow from the LOW SIDE NETWORK to the HIGH SIDE NETWORK via the DATA DIODE DEVICE.

User refers to the person who utilizes the Interactive Link in performance of duties.

Window Server refers to a system that communicates with a USER on behalf of a Window Management System. A WINDOW SERVER may be a terminal, such as an X-Terminal, or a Workstation running a WINDOW SERVER Program.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.
- *Interactive Link Common Criteria Security Target, Issue 12.2,* 12 August, 2005.
- *Tenix Interactive Link Version 5.1 Evaluation Technical Report,* July 15, 2005.
- *Test Report for a Target of Evaluation, Tenix Interactive Link version 5.0,* August 24th, 2004.

- *Penetration Test Report for a Target of Evaluation, Tenix Interactive Link version 5.0,* August 26th, 2004.
- *ETR sections for NSA evaluation effort*