Owl Computing Data Diode
Common Criteria Security Target
(EAL2)

Version 4.0

Prepared for

Owl Computing Technologies, Inc.
19 North Salem Road (2nd Floor)
P.O. Box 313
Cross River, N.Y. 10518

Owl Computing
Technologies

Prepared by

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

October 31, 2002

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

OWL COMPUTING TECHNOLOGY

1 REVISION HISTORY

This Section provides a mechanism to identify when specific versions of this document were released and also specifies what modifications were performed when moving from one version to the next.

Version	Date	Comments
1.0	21 September 2000	Initial draft
1.1	23 April 2002	Second draft
1.2	5 May 2002	Third Draft – minor revision
1.3	24 June 2002	Final CC evaluation draft
2.0	1 August 2002	Final submitted for evaluation.
3.0	30 October 2002	Final – accepted by NIAP
4.0	31 October 2002	Final -

2 SECURITY TARGET INTRODUCTION

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. This ST describes a set of security requirements and specifications to be used as the basis for evaluation of an identified Information Technology (IT) product. The IT product described in this ST is the Data Diode Network Interface Card (NIC), herein called the Data Diode NIC, developed by Owl Computing Technologies Incorporated, herein called Owl. The Data Diode NIC components are the subject of an evaluation and are called the Target of Evaluation (TOE).

The Owl Data Diode NIC ensures an information flow policy where unidirectional optical fiber communication is enforced between two gateways (i.e., host machines). Data Diodes are installed in pairs where there is a receive-only Data Diode NIC and a send-only Data Diode NIC. Each Data diode NIC is installed into a host.

All information flow from one gateway must flow into a receive-only Data Diode NIC that is physically and logically restricted to only receive network traffic and cannot send network traffic. All traffic received is passed directly to the connected host. All information flow from the Data Diode NIC to a gateway must flow through a send-only Data Diode NIC that is physically and logically restricted from receiving traffic. All traffic that is sent through the send-only Data Diode NIC is sent at the request of the connected host.

Once manufactured, there is no way to alter the function of a Data Diode NIC.

The Security Target contains the following additional sections:

Section	Topic
2.	Introductory material for the ST.
3.	TOE description.
4.	Expected environment for the TOE
5.	Security objectives for both the TOE and the TOE environment
6.	Functional and assurance requirements
7.	Security functions, assurance measures, and assurance evidence
8.	Claims of compliance for a specific Protection profile.
9.	Rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats.

2.1 Security Target, TOE, and CC Identification

The following summary information identifies this ST and the TOE:

Evaluation (TOE): the Data Diode network interface card (NIC),
Evaluation Assurance Level: (EAL) 2,
ST Title: Owl Computing Technologies Incorporated, Data Diode Security Target,
ST Version: 4.0,
TOE Identification: Data Diode – Version 1, Data Diode – Version 2
CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999,
ST Author: Science Applications International Corporation (SAIC)

2.2 Conformance Claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
  - Part 2 conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.

- Part 3 conformant

2.3 Strength of Environment

The Owl Data Diode NIC provides for a level of protection that is appropriate for IT environments that require one-way information flow where the Data Diode can be appropriately protected from hostile attacks. The assurance requirements, EAL2, were chosen to be consistent with this environment.

2.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

2.4.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2.4.2 Terminology and Acronyms

The following terms and acronyms are used in this Security Target:

ATM PHY. The ATM PHY is a high performance physical layer inter-face chip on the Data Diode NIC that generates and receives high-speed data streams. The ATM PHY receives 53-byte ATM cells from the SAR and produces analog signals that are passed to the transceiver. The interface into the ATM PHY from the SAR uses the UTOPIA protocol and the interface to the transceiver is SONET over analog power pins.

CC. Common Criteria for Information Technology Security Evaluation

Data Diode. A network interface card consisting of three functional components; the "Segmentation and Reassembly Component (SAR)", the ATM physical packet interface chip (PHY), and the fiber optic communication interface (transceiver). These components are purchased from Integrated Device Technologies as a complete integrated card; then, the transceiver is modified by Owl to restrict communication to always receive or always send.

Data Diode Host. A network connected host where the network connections are provided by a single photodiode to send or a single light detector to receive.

EAL. Evaluation Assurance Level

Gateway. Also called a router, a gateway is a program or a special-purpose host that transfers network traffic with an identifiable network address from one network to another until the final destination is reached.

Host. A general term for a computer system. Once specific application software or hardware is installed on a host it assumes the role of Data Diode Host, gateway, receiving Host, Sending Host.

NIC. Network Interface Card that provides the physical interface to a network.

PCI Bus Interface. The Peripheral Component Interconnect bus interface is the device driver interface into the TOE from the host computer. The PCI Bus is an open architecture bus structure to control devices. Composed of a PCI BIOS, CPU, CPU cache, system cache, system memory, PCI Bridge, and Peripheral bus.

Receive-only Data Diode. An ATM SAR controller for PCI-based networking applications integrated circuit card that has been permanently modified by Owl so that the transceiver has no light source but does have a photo-detector.

Receiving Host. A host receiving network traffic though a receive-only Data Diode NIC that receives traffic from the network using a light detector to receive light impulses through a fiber-optic cable.

SAR. The Segmentation and Reassembly (SAR) chip on the Data Diode NIC accepts buffers information from the Peripheral Component Interconnect (PCI) bus interface on a host computer and produce complete 53-byte ATM cells from the buffered information it receives. These cells are sequential packets for the ATM physical packet interface chip (PHY).

Sending Host. A host sending network traffic though a send-only Data Diode NIC that sends traffic over the network using a photodiode to send light impulses through a fiber-optic cable.

Send-only Data Diode
An ATM SAR controller for PCI-based networking applications integrated circuit card that has been permanently modified by Owl so that the transceiver has no photo-detector but does have a light source.

SONET Protocol
The interface between the ATM PHY and the transceiver provides both Transmission Convergence (TC) and Physical Media Dependent (PMD) sub-layer functions of an ATM PHY suitable for ATM networks.

UTOPIA Protocol
The UTOPIA (Universal Test and Operations PHY Interface for ATM) interface is the protocol used between the SAR and the ATM PHY. UTOPIA is a standard data path handshake protocol.

3 TOE DESCRIPTION

The Data Diode NIC is designed and manufactured by Owl Computing Technologies Incorporated located at 19 North Salem Road (2nd Floor) P.O. Box 313 Cross River, N.Y. 10518 U.S.A., herein called Owl.

The TOE is a pair of Data Diode NIC network interface cards. Each card has two external interfaces. One external interface is the PCI Bus of the host in which the Data Diode NIC is installed. The other interface is the fiber optic network connection physically located on the card. Each Data Diode NIC has two network connections, one for incoming traffic, and one for outgoing traffic, however only one connection can be active for one type of card, therefore it requires a pair of Data Diode NIC cards to communicates from a sending host to a receiving host. The purpose for the Data Diode NIC is to provide assurance of one-way operation occurs at the physical interface between a network sender and receiver. Enabling only a single photodiode on the sender and a single light detector on the receiver insures one-way information flow over a fiber-optic line. A machine cannot have both a send and a receive card. The Data Diode NIC is provided in two models, the send-only and receive-only NICs.

This Data Diode NIC was developed to support higher-level application software packages to provide secure one-way network communications. Owl markets and sells application programs that utilize the Data Diode Technology for specific data transfers, however only the TOE is the Data Diode NIC.

The information flow policy enforced by the Data Diode NIC does not rely on passwords, authentication, or encryption to protect host data. Rather the physics of a photo-detector and light emitting diode enforce the TSP.

3.1 Product Type

The Owl Data Diode NIC is a physical network interface card that physically plugs into the PCI Bus of a host computer and has connectors built on the card for fiber-optic connections to a network. The card has three chips on it.

3.2 Product Description

The Target of Evaluation (TOE) is either one of two versions of the Data Diode NIC hardware card offered by Owl. The difference in Version 1 and Version 2 of the TOE is strictly limited to throughput. Either version of the TOE is offered as a single Data Diode as a send-only NIC or as a receive-only NIC, or as a pair of Data Diode NICS for two-way communication. Owl uses a proprietary protocol to translate light impulses into data, however the protocol is not part of the TOE and is not required to meet the TSF. Any host that supports a PCI Bus is sufficient for the correct operation of the TSF; therefore the host is not part of the TOE.

A pair of Data Diode NIC cards is required to move packet data directly between a send-only communication card and a receive-only communication card. The data is formatted, framed and queued in the "Send-Only Communication Card" once across the PCI Bus. The output of the "Send-Only Communication Card" is a fiber optic cable connected to a "Receive-Only Communication Card". Data is then transferred from the "Receive-Only Communication Card" across the PCI Bus, for availability to application programs.

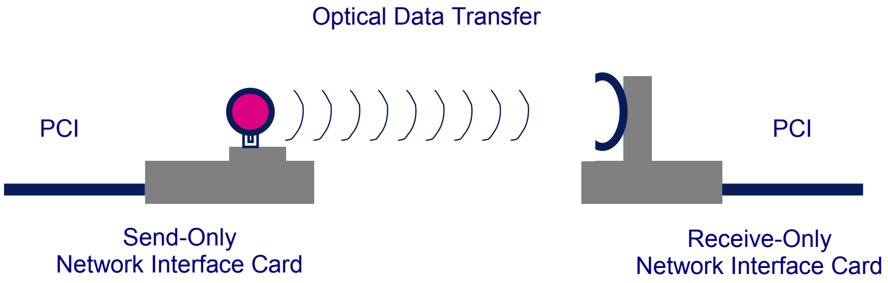

Figure 1 - High Level view of the Data Diode Interface

The Data-Diode interface provides an absolute one-way connection between the sender and the receiver. It consists of a send-only communication card and a receive-only communication card. The purpose is to insure that no communications can originate from the receive-only communication card back to the send-only communication card.

The TOE consists of a send-only optical communication card and a receive-only optical communication card whereby packets of data move uni-directionally from a send-only optical communication card to a receive-only communication card. The data is staged, queued, segmented and framed in the "Send-Only Communication Card" for packet transfers across the PCI Bus. The output of the "Send-Only Communication Card" is an optical photo-diode, which transfers information by way of a fiber optic cable connected to optical receiver in the "Receive-Only Communication Card". Data packets are then received with a photo-detector and reassembled into the original message by the "Receive-Only Communication Card".

3.3 Security Environment TOE Boundary

The Target of Evaluation (TOE) is comprised of two Data Diode integrated circuit cards. Each circuit card connects to a standard PCI slot in a computer and each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode card is receive-only in that the computer system in which the receive-only card resides can only exchange data with the card by issuing some form of read request. The other Data Diode card is send-only in that the computer system in which the card resides can only exchange data with the by issuing a write request.

The components that are necessary to create a Data Diode are purchased from Integrated Device Technologies as a complete integrated card. The card is then modified to create the two types of Data Diode cards. The SAR and the ATM PHY components are identical in both types of Data Diode cards. It is the transceiver that defines the Data Diode type, and it is the transceiver that provides the TOE Security Function (TSF). The assurance of one-way operation occurs at the physical interface between the sender and receiver. A send-only Data Diode has a single photodiode active in the transceiver while a receive-only Data Diode has a single light detector active in the transceiver.

3.3.1 Physical Boundary

An itemized list of the TOE follows. Added to the list of TOE components are documents and the additional material that will be evaluated to determine that the TOE meets the EAL2 level of assurance.

The Target of Evaluation (TOE) is comprised of two Data Diode NIC integrated circuit cards. Each card is connected to a standard PCI slot in a computer. Each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode NIC is a send-only card, and the other type of data diode

NIC is a receive-only card. Both types of cards are modified ATM Segmentation and Reassembly integrated card for PCI-based networking applications – Model IDT77211.

Each Data Diode NIC has two external interfaces. Each type of Data Diode NIC (receive-only, and send-only) has a Peripheral Component Interconnect (PCI) bus interface that accepts buffers of information from the host (send-only) or puts buffers of information on the PCI Bus for the host (receive-only). The data and control information from the PCI Bus to the Data Diode NIC are received by the ATM Segmentation and Reassembly (SAR) controller. The SAR connects directly to the PCI Bus and exchanges data and control information between the PCI Bus and the TOE. The SAR uses host memory to change packet (buffered) information that is receives from the PCI Bus interface and serializes the byte stream for the ATM Phy chip, an internal TOE subsystem. The ATM SAR also receives a serial byte stream from the ATM Phy and blocks the data into a buffered packet format before placing packets on the PCI Bus. Although the SAR is part of the TOE and exports an interface to PCI Bus, the SAR provides no TSF.

Each type of Data Diode NIC card has a transceiver that physically provides two ports for a network fiber-optic connection. There is one receive port and one send port. The send port exports light pulses to a receive port that receives light impulses. To export light pulses over the send port, the transceiver converts electrical voltage received over an internal TOE interface into light impulses. To import light pulses over the receive port; the transceiver converts light impulses into electrical voltage that are sent over an internal TOE interface.

3.3.2 Logical Scope and Boundary

The Data Diode provides a way for information from a source computer to be sent to a destination computer in a fast (155 Mbps), one-way data stream.

The Target of Evaluation (TOE) is comprised of two Data Diode NIC integrated circuit cards. Each card is connected to a standard PCI slot in a computer. Each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode card is receive-only in that the computer system in which the receive-only card resides can only exchange data with the card by issuing some form of read request. The other Data Diode card is send-only in that the computer system in which the card resides can only exchange data with the by issuing a write request.

The Data Diode NIC enforces the information flow policy that only one-way communication can ever occur across a port connecting two hosts by hand modifying a commercial commodity two-way ATM communication cards to insure that only unidirectional data transfer is provided. For all receive-only cards the power to the light source on the transceiver is disconnected and the transmit port is permanently rendered inoperable. For all send-only cards, the power to the photo-diode is permanently disconnected and the receive port is permanently rendered inoperable.

3.3.2.1 Information Flow Protection

A Data Diode NIC physically can only provide network traffic flow in one direction over any single network connection and this TSP is enforced at the physical level. One send-only Data Diode NIC communicating with a receive-only Data Diode NIC is required for communication between them over the ports that they are exporting. [1]

If a host attempts to send traffic over a receive-only Data Diode NIC, buffers of data may be sent through the host device driver over the PCI Bus to the receive-only Data Diode NIC. The receive-only NIC will process the buffer, and convert binary to voltage, and voltage into light impulses. But when transceiver goes to transmit the light impulses, there is no light source since it has been physically disconnected. Also the send port has been physically blocked so that no light impulses can be transmitted. When the host does not receive a response from a connection request, it is up to the host protocol to deal with no response to

[1] Communication between hosts over other ports through network connections other than the TOE is outside the scope of this Security Target.

the connection request. The TSF is maintained even though the host has attempted to send information through a receive-only Data Diode NIC.

If a host attempts to listen for traffic over a send-only Data Diode NIC, no signals/bits/buffers/voltage will be received by the device driver listening on the PCI Bus for data from the send-only Data-Diode NIC. The send-only Data Diode NIC has had the photodiode physically disconnected. Also the receive port has been physically blocked so that no light impulses can be received. When the host does not receive a response while listening for data from the send-only Data Diode NIC, it is up to the host protocol to deal with no data. The TSF is maintained even though the host has attempted to receive information through a send-only Data Diode NIC.

3.3.2.2 TOE Self Protection

The Data Diode NIC protects itself by not exporting an interface that can modify the TOE. The only interfaces exported are the PCI Bus interface and the network fiber optic interface. Neither interface can alter the TSF since the TOE has been physically modified to enforce the TSF and the TOE would have to be physically modified to violate the TSF. Since the TOE environment does not allow tampering with the host device in such a way that the Data Diode NIC can be removed by anyone other than an administrator, it is physically impossible to modify the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic.

4 SECURITY ENVIRONMENT

The TOE security environment consists of the threats to security, organizational security policies, and usage assumptions as they relate to the Data Diode NICs.

Data Diode NICs provides for a level of protection that is appropriate for IT environments that require strict control over directional information flow across a network. A Data Diode NIC is not designed to withstand physical attacks directed at disabling or bypassing its security features, however it is designed to withstand logical attacks originating from its attached network. Data Diode NICs are suitable for use in both commercial and government environments.

4.1 Threats to Security

Threats are undesirable events and are characterized in terms of a threat agent, a presumed attack method, vulnerabilities that are the foundation for the attack, and identification of the asset under attack.

Threat agents are of two types. One, are individuals who have not been granted physical access to the workstation gaining physical access. Two, a subject executing on a workstation, in which the TOE in installed, attempting to cause an information flow contrary to the direction of the information flow established when the TOW was installed.

Assets comprise the data transmitted between a send NIC and a receive NIC, such that uni-directional transmission must be maintained over a connection.

In general, the ***threat agents*** are assumed to have an attack potential of ***low***. As a result, the TOE has been developed with the assumption that a potential attacker would have a proficient level of expertise, access to public knowledge of the TOE, restricted access to the TOE, have access to standard equipment and also have a low-level of motivation.

The security threats facing the TOE are listed in Table 1.

Table 1 - Security Threats

Name (T = Threat)	**Threat**
T.FULL_DUPLEX	If the receive photodiode on a Send-only NIC can sense light from the light source, then a subject executing on a workstation, in which the TOE in installed, could cause an information flow contrary to the direction of the information flow established when the TOE was installed.
T.INCORRECT_FLOW	A Receive-Only Data Diode NIC can receive a send request over the PCI Bus to send information. A Send-Only Data Diode NIC can receive a listen-on-this-port request over the PCI Bus. A NIC that allows requests from the PCI Bus that are inconsistent with the direction of the information flow, could cause an information flow contrary to the direction of the information flow established when the TOE was installed.
T.TAMPERING	A person, with sufficient time, tools [e.g., soldering iron, wire, propane torch, new physical network connectors], and access to the TOE, can change the information flow through a Data Diode NIC and violate the policy.

The only TOE Security Feature (TSF) is that the photo-detector on the receive-only Data Diode NIC will turn itself into a light source and that the light source on the send-only Data Diode NIC cannot detect light from another source. This can be assured by basic electronic device physics and this design is unique in the security industry today.

4.2 Organization Security Policy

P.OneWay The TOE will ensure that information can only flow in one direction between hosts when communicating is provided by Data Diode NICs.

4.3 Secure Usage Assumptions

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include both practical realities in the implementation of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 - Secure Usage Assumptions

Type	**Name** **(**A = Assumption)	**Assumption**
Physical	A.PHYSICAL	The TOE is physically secure.
Physical	A.CONNECTION	A protected fiber optic connection exists between any pair Data Diode NICs
Host	A.ADMIN	Only a trained trusted administrator installs the TOE into a host.
Personnel	A.NOEVIL	Authorized administrators and installers are non-hostile.

5 SECURITY OBJECTIVES

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either TOE security objectives or environment security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats, assumptions, and organizational policies are addressed under one of the categories below.

5.1 TOE Security Objectives

The following are the TOE's IT security objectives:

Table 3 - TOE Security Objectives

Objective	**Description**
O.HOST_INSTRUCTION	The direction of the information flow through a Data Diode NIC cannot be altered by an instruction from a higher-level abstraction (e.g. operating system, application).
O.READ_ONLY	A permanent condition exists whereby information that can be received by a Data Diode NIC installed on a host can be read by an executing abstraction attempting to read from that host connection, but an executing abstraction cannot write over the same connection.
O.WRITE_ONLY	A permanent condition exists whereby information that can be sent by a Data Diode NIC installed on a host can be written by an executing abstraction attempting to write to the host connection, but an executing abstraction cannot read over the same connection.
O.PHYSICAL_LEVEL_ENFORCEMENT	The TSP is enforced at the physical level and is unaware of higher-level abstractions.

5.2 Environmental Security Objectives

Certain objectives with respect to the general operating environment must be met. The following are the TOE's environmental security objectives

Table 4 - Environmental Security Objectives

Objective	**Description**	**Assumptions & Threats**
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, and operated in a manner that maintains IT security.	A.ADMIN A.NOEVIL T.FULL_DUPLEX
OE.NETWORK	Two protected fiber-optic network connections are required for an exchange of information. One send and one receive connection is required for information to flow over a connection[2].	A.CONNECTION
OE.BENIGN	Administrators and users will not knowingly attempt to subvert security features.	A.NOEVIL A.PHYSICAL
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	A.ADMIN A.PHYSICAL

6 IT SECURITY REQUIREMENTS (ASE_REQ)

This section defines the detailed IT security requirements that are satisfied by the TOE or its environment. TOE security requirements shall be stated as follows:

1. **TOE security functional requirements (SFRS)** are defined as functional components drawn from Part 2 where applicable. The TOE meets all the SFRS claimed in the next section.
2. **TOE security assurance requirements (SARS)** are defined as the assurance components drawn from Part 3 of the CC where applicable. The TOE meets all SARS required for EAL2.
3. The optional statement of **security requirements for the IT environment** identifies the IT security requirements that are to be met by the IT environment of the TOE.

These requirements are discussed in separate sub-sections within this section. For specific requirements, there are no refinements or iterations included in the ST.

6.1 TOE CC Security Functional Requirements (SFRs)

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria.

Table 5 - Functional Components lists the IT functional requirements and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 8 have been satisfied.

Table 5 - Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FDP_IFC.2.	Complete information flow Control	FDP_IFC.1	FDP_IFF.1	O.HOST_INSTRUCTION O.PHYSICAL-LEVEL-ENFORCEMENT
FDP_IFF.1	Simple security Attributes	None	FDP_IFC.1 FMT_MSA.3[3]	O.READ_ONLY O.WRITE_ONLY
FPT_RVM.1	Non-Bypassability of the TSF	None	None	O.HOST_INSTRUCTION O.READ_ONLY O.WRITE_ONLY
FPT_SEP.1	TSF domain separation	None	None	O.PHYSICAL-LEVEL-ENFORCEMENT

The functional requirements in the above table are described below in further detail. They are derived verbatim from the Common Criteria Version 2.1 Part 2, with the exceptions whereby the operations “assignment” is completed using the conventions identified in Section 2.4.1.

6.1.1 Information flow control policy (FDP_IFC)

6.1.1.1 FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1

[2] The management policy is purely environmental and its protection is purely physical (i.e., both outside the scope of the TOE and its SFPs). Once the TOE is installed into a host, no management action is necessary or possible.

6.1.1.1.1 FDP_IFC.2.1

The TSF shall enforce the **[assignment: unidirectional information flow SFP]** on **[assignment: any request from an external interface to move data packets through the TOE]** and all operations that cause that information to flow to and from subjects covered by the SFP.

6.1.1.1.2 FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple security attributes

6.1.2 Information flow control functions (FDP_IFF)

6.1.2.1 FDP_IFF.1-NIAP-0407 Simple security attributes

Hierarchical to: No other components.

6.1.2.1.1 FDP_IFF.1.1

The TSF shall enforce the **[assignment: the unidirectional information flow SFP]** based on the following types of subject and information security attributes **[assignment: physical transceiver configuration of each Data Diode]**.

6.1.2.1.2 FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) **If the physical transceiver configuration of the data Diode permits it to send data, then the sending of data packets is permitted.**

b) **If the physical transceiver configuration of the data Diode permits it to receive data, then the receiving of data packets is permitted.**

6.1.2.1.3 FDP_IFF.1.3-NIAP-0407

The TSF shall enforce the following information flow control rules: ***[selection: no additional information flow control SFP rules]***.

6.1.2.1.4 FDP_IFF.1.4-NIAP-0407

FDP_IFF.1.4 The TSF shall provide the following: ***[selection: no additional SFP capabilities]***.

6.1.2.1.5 FDP_IFF.1.5-NIAP-0407

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: ***[selection: no explicit authorization rules].***

6.1.2.1.6 FDP_IFF.1.6-NIAP-0407

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***[selection: no explicit denial rules]***.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FMT_MSA.3 does not apply since the TOE provides a fixed information flow policy that cannot be modified. For further discussion see Section 9.

6.1.3 Reference mediation (FPT_RVM)

6.1.3.1 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

6.1.3.1.1 FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

6.1.4 Domain separation (FPT_SEP)

6.1.4.1 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

6.1.4.1.1 FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

6.1.4.1.2 FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies: No dependencies.

Dependencies: No dependencies.

6.2 Security Functional Requirements for the IT Environment

There are no security functional requirements (SFRs) are intended to be satisfied by the IT environment rather than the TOE itself. All SFRs were drawn from Part 2 of the Common Criteria

6.3 Security Assurance Requirements (SARs)

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 6 identifies the EAL 2 assurance requirements and the assurance class. All assurance dependencies associated with the components in Table 9 have been satisfied.

Table 7 - EAL2 Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration items
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Tests (ATE)	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6.3.1 Configuration Management (ACM)

6.3.1.1 Configuration Items (ACM_CAP.2)

6.3.1.1.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

6.3.1.1.2 ACM_CAP.2.3D

The developer shall provide CM documentation.

6.3.1.1.3 ACM_CAP.2.1C

The reference for the TOE shall be unique to each version of the TOE.

6.3.1.1.4 ACM_CAP.2.2C

The TOE shall be labeled with its reference.

6.3.1.1.5 ACM_CAP.2.3C

The CM documentation shall include a configuration list. The configuration list shall uniquely identify all configuration items that comprise the TOE.

6.3.1.1.6 ACM_CAP.2.RI-3

The configuration list shall uniquely identify all configuration items that comprise the TOE

6.3.1.1.7 ACM_CAP.2.4C

The configuration list shall describe the configuration items that comprise the TOE.

6.3.1.1.8 ACM_CAP.2.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

6.3.1.1.9 ACM_CAP.2.6C-NIAP-0412

The configuration list shall uniquely identify all configuration items

6.3.1.1.10 ACM_CAP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.2 Delivery and Operation (ADO)

6.3.2.1 Delivery Procedures (ADO_DEL.1)

6.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

6.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

6.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

6.3.2.1.4 ADO_DEL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

6.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

6.3.2.2.2 ADO_IGS.1.1C – RI-51

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

6.3.2.2.3 ADO_IGS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

6.3.3 Development (ADV)

6.3.3.1 Fully defined external interfaces (ADV_FSP.1)

6.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

6.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

6.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

6.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

6.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

6.3.3.1.6 ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

6.3.3.2 Security enforcing high-level design (ADV_HLD.1)

6.3.3.2.1 ADV_HLD.1.1D

The developer shall provide the high level design of the TSF.

6.3.3.2.2 ADV_HLD.1.1C

The presentation of the high level design shall be informal.

6.3.3.2.3 ADV_HLD.1.2C

The high level design shall be internally consistent.

6.3.3.2.4 ADV_HLD.1.3C

The high level design shall describe the structure of the TSF in terms of subsystems.

6.3.3.2.5 ADV_HLD.1.4C

The high level design shall describe the security functionality provided by each subsystem of the TSF.

6.3.3.2.6 ADV_HLD.1.5C

The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

6.3.3.2.7 ADV_HLD.1.6C

The high level design shall identify all interfaces to the subsystems of the TSF.

6.3.3.2.8 ADV_HLD.1.7C

The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

6.3.3.2.9 ADV_HLD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.3.2.10 ADV_HLD.1.2E

The evaluator shall determine that the high level design is an accurate and complete instantiation of the TOE security requirements.

6.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

6.3.3.3.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

6.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

6.3.3.3.3 ADV_RCR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.4 Guidance Documents (AGD)

6.3.4.1 Administrator Guidance (AGD_ADM.1)

6.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

6.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

6.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

6.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

6.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

6.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

6.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

6.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documents supplied for evaluation.

6.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

6.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

6.3.4.2 User Guidance (AGD_USR.1)

6.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

6.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

6.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

6.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

6.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

6.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

6.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

6.3.4.2.8 AGD_USR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5 Security Testing (ATE)

6.3.5.1 Analysis of coverage (ATE_COV.1)

6.3.5.1.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

6.3.5.1.2 ATE_COV.1.1C

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

6.3.5.1.3 ATE_COV.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5.2 Functional testing (ATE_FUN.1)

6.3.5.2.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

6.3.5.2.2 ATE_FUN.1.2D

The developer shall provide test documentation.

6.3.5.2.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

6.3.5.2.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

6.3.5.2.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

6.3.5.2.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

6.3.5.2.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

6.3.5.2.8 ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5.3 Independent testing – sample (ATE_IND.2)

6.3.5.3.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

6.3.5.3.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

6.3.5.3.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

6.3.5.3.4 ATE_IND.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5.3.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

6.3.5.3.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

6.3.5.4 Strength of TOE security function evaluation (AVA_SOF.1)

6.3.5.4.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

6.3.5.4.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

6.3.5.4.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

6.3.5.4.4 AVA_SOF.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5.4.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

6.3.5.5 Developer analysis (AVA_VLA.1)

6.3.5.5.1 AVA_VLA.1.1D – RI-51

The developer shall perform a vulnerability analysis.

6.3.5.5.2 AVA_VLA.1.2D – RI-51

The developer shall provide vulnerability analysis documentation.

6.3.5.5.3 AVA_VLA.1.1C – RI-51

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

6.3.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

6.3.5.5.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

6.3.5.5.6 AVA_VLA.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5.5.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

7 TOE SUMMARY SPECIFICATION (ASE_TSS)

This section describes the security functions and associated assurance measures.

7.1 TOE Security Functions

This section presents the security functions performed by the TOE. To aid evaluation of the TOE, security functions are mapped to SFRs.

7.1.1.1 Information Flow Control

A Data Diode NIC physically can only provide network traffic flow in one direction over any single network connection and this TSP is enforced at the physical level. One send-only Data Diode NIC communicating with a receive-only Data Diode NIC is required for communication between them over the ports that they are exporting.[4]

If a host attempts to send traffic over a receive-only Data Diode NIC, buffers of data may be sent through the host device driver over the PCI Bus to the receive-only Data Diode NIC. The receive-only NIC will process the buffer, and convert binary to voltage, and voltage into light impulses. But when transceiver goes to transmit the light impulses, there is no light source since it has been physically disconnected. Also the send port has been physically blocked so that no light impulses can be transmitted. When the host does not receive a response from a connection request, it is up to the host protocol to deal with no response to the connection request. The TSF is maintained even though the host has attempted to send information through a receive-only Data Diode NIC.

If a host attempts to listen for traffic over a send-only Data Diode NIC, no signals/bits/buffers/voltage will be received by the device driver listening on the PCI Bus for data from the send-only Data-Diode NIC. The send-only Data Diode NIC has had the photodiode physically disconnected. Also the receive port has been physically blocked so that no light impulses can be received. When the host does not receive a response while listening for data from the send-only Data Diode NIC, it is up to the host protocol to deal with no data. The TSF is maintained even though the host has attempted to receive information through a send-only Data Diode NIC.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.2
- FDP_IFF.1
- FDP_RVM.1

7.1.1.2 TOE Self Protection

The Data Diode NIC protects itself by not exporting an interface that can modify the TOE. The only interfaces exported are the PCI Bus interface and the network fiber optic interface. Neither interface can alter the TSF since the TOE has been physically modified to enforce the TSF and the TOE would have to be physically modified to violate the TSF. Since the TOE environment does not allow tampering with the host device in such a way that the Data Diode NIC can be removed by anyone other than an administrator, it is physically impossible to modify the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic. The Target of Evaluation

[3] Communication between hosts over other ports through network connections other than the TOE is outside the scope of this Security Target.

(TOE) is comprised of two Data Diode integrated circuit cards that are each connected to a standard PCI slot in a computer and are connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode card is receive-only in that the computer system in which the receive-only card resides can only exchange data with the card by issuing some form of read request. The other Data Diode card is send-only in that the computer system in which the card resides can only exchange data with the by issuing a write request.

The TOE Self Protection function is designed to satisfy the following security functional requirements:

- FPT_SEP.1
- FDP_IFF.1

7.2 Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

7.2.1 Configuration Management

This section identifies the Configuration Management, measures associated with the TOE.

The Configuration Management measures applied by Owl specifically identify the TOE and the measures that control all configuration management activities necessary to fully control the design, planning, implementation, testing, fielding and documentation of the TOE

The configuration management system is described in the document, ***Owl Data Diode Configuration Management Plan*.**

Acceptance procedures are identified in paragraphs 3 and 4 of the second section in chapter 2 in the Secure Directory File Transfer System OEM Install User's Manual. Chapter 2 is titled, "Installation," and the second section of that chapter is titled, "Hardware Configuration that are to be executed at the customer site to ensure the TOE is installed correctly are described in the ***Owl Data Diode Installation Guide***.

Assurance Requirements Satisfied: ACM_CAP.2 (Configuration items).

7.2.2 Delivery and Operation

The delivery and operation of the TOE is controlled sufficiently to ensure that the TOE is installed, generated, and started in the same way the designer and installer intended it to be and that it is delivered without modification. This includes both the procedures taken while the TOE is in transit, as well as the installation procedures.

Owl provides delivery and installation documentation in the first two sections of chapter 2 in the Secure Directory File Transfer System OEM Install User's Manual. Chapter 2 is titled, "Installation," and the first section in that chapter is titled, "Components of the System," and the second section is titled, "Hardware Configuration.

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1; and
- ADO_IGS.1.

7.2.3 Administrator and User Guidance

There is no untrusted user interface into the TOE; therefore guidance to be provided to an untrusted user does not apply.

The Common Criteria appears to separate installation of the TOE from administration. Installation is the process of configuring the TOE at start-up before it is placed in an operational state. Administration, according to the CC, is the process of maintaining configuration settings and data on which security policy decisions depend once the TOE is operational. Unfortunately, the separation of administration from installation is not always clear. Even so, the introductory material to the ADO_IGS requirement in Part 3 of the CC states, "The installation, generation, and start-up procedures may exist as a separate document or could be grouped with other administrative guidance. The requirements in this assurance family are presented separately from those in the AGD_ADM family, due to the infrequent, possibly one-time use of the installation, generation and start-up procedures." The TOE provides no configurable settings or options available to a customer. Once the TOE is physically installed in a host, it is operational and no further administration is necessary. Indeed, the TOE provides no administrator interface before installation or once installed, therefore the assurance requirement for administrative guidance is satisfied by the ADO_IGS assurance requirement.

For the reasons sited in this section, the Secure Directory File Transfer System OEM Install User's Manual satisfies the following Assurance requirements:

- AGD_ADM.1
- AGD_USR.1

7.2.4 Development

The development assurance components for EAL2 have been completed by Owl. These components include: informal functional specification, descriptive high-level design, and an informal correspondence demonstration.

- ADV_FSP.1: Section 2 of the Secure Directory File Transfer System (DFTS) document, titled "Secure DFTS," includes a subsection, titled "Physical Modifications." This subsection fully describes the TSF.
- ADV_HLD.1: The *"High Level Interface Description (EAL2)"* satisfies the requirement for decomposing the TOE into subsystems and fully describes each subsystem, including inter-subsystem interfaces.
- ADV_RCR.1: The Data Diode System EAL Common Criteria Informal Correspondence Document provides the correspondence between the various design documentation is implicit to the way in which the documentation is structured. The way that this correspondence is evident within the design documentation is:
    - ST-TSS to FSP: The Data Diode System EAL Common Criteria Informal Correspondence Document describes how the interfaces correspond with the security functions in the ST.

  - FSP to HLD: The EAL Common Criteria Low-Level Design Reference Document describes how the various security behavior in the Owl Data Diode NIC's Functional Specification are further refined.

7.2.5 Tests

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1 Owl has completed an analysis of test coverage to determine that all tests identified and the TSF described in the functional specification are tested. The document that describes test coverage is the *Testing the Security Features of the Data Diode.*

- ATE_FUN.1: Owl had the Data Diode NIC functionally tested by Sandia Laboratories. The *Test Report* from that testing effort describes test plan (Reason for testing), test procedure descriptions and expected test results (Test Summary) and actual test results, the security functions to be tested and describe the goal of the tests to be performed.

- ATE_IND.2: The TOE and test documentation will be available for independent testing.

7.2.6 Vulnerability Analysis

Owl performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. The *Test Report* that documents the independent testing performed by Sandia Laboratories identifies potential vulnerabilities whereby the photo-detector could, under extreme circumstances, emit light. The possibility of this occurring and the remedy to thwart this vulnerability are discussed.

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_VLA.1.

Note: AVA_SOF does not apply to the TOE, since there are no permutational or probabilistic mechanisms to meet a SOF claim.

8 PROTECTION PROFILE CLAIMS

There are no Protection Profile claims made for the TOE.

9 RATIONALE

Each subsection in Section 7, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security function and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

9.1 Security Objectives Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

9.1.1 Security Objectives for the Environment Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

Table 8 - Mapping Security Objectives to Environment

Objectives	O.HOST_INSTRUCTION	O.READ_ONLY	O.WRTE_ONLY	O.PHYSICAL_LEVEL_ ENFORCEMENT	OE.BENIGN	OE.NETWORK	OE.PHYSICAL
T.Full_Duplex	X						
T.Incorrect_Flow		X	X				
T.Tampering				X			
P.OneWay	X	X	X				
A.Admin					X		
A.Connection						X	
A.Noevil					X		X
A.Physical							X

9.1.1.1 T_FULL_DUPLEX

If the receive photodiode on a Send-only NIC can sense light from the light source, then a subject executing on a workstation, in which the TOE in installed, could cause an information flow contrary to the direction of the information flow established when the TOW was installed.

This threat is countered by ensuring each Data Diode NIC is correctly modified, identified, and correctly installed. A Data Diode NIC physically can only provide network traffic flow in one direction over any single network connection and this TSP is enforced at the physical level. [O.Host_Instruction]

9.1.1.2 T_INCORRECT_FLOW

A Receive-Only Data Diode NIC can receive a send request over the PCI Bus to send information. A Send-Only Data Diode NIC can receive a listen-on-this-port request over the PCI Bus. A NIC that allows requests from the PCI Bus that are inconsistent with the direction of the information flow, could cause an information flow contrary to the direction of the information flow established when the TOE was installed.

This threat is countered by ensuring that:
If an instruction is received from the PCI Bus interface that requests an incorrect information flow, the TOE is physically incapable of executing the instruction. Regardless of the information flow request from the host, the physical communication limitations on the Data Diode NIC prevents the host from initiating an information flow that violates the TSP [O.Read_Only, and O.Write_Only].

9.1.1.3 T.TAMPERING

A person, with sufficient time, tools [e.g., soldering iron, wire, propane torch, new physical network connectors], and access to the TOE, can change the information flow through a Data Diode NIC and violate the policy.

This threat is countered by ensuring that:
The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic [O.Physical_Level_Enforcement].

9.1.1.4 P.OneWay

The TOE will ensure that information can only flow in one direction between hosts when communicating is provided by Data Diode NICs.

This policy is provided by fact that the direction of the information flow through a Data Diode NIC cannot be altered by an instruction from a higher-level abstraction (e.g. operating system, application) because the enforcement of the TSP is provided by permanent physical alteration of the TOE [O.Host_Instruction, O.Read_Only, and O.Write_Only].

9.1.1.5 A.Admin

Only a trained trusted administrator installs the TOE into a host.

This assumption is met by:
Those responsible for the TOE must ensure that the TOE is installed by administrators who will not attempt to subvert the security features, and operated in a manner that maintains IT security [OE.Benign, OE.Install].

9.1.1.6 A.Connection

A protected fiber optic connection exists between any pair Data Diode NICs

This assumption is met by:
Two protected fiber-optic network connections are required for an exchange of information. One send and one receive connection is required for information to flow over a connection [OE.Network.

9.1.1.7 A.Noevil

Authorized administrators and installers are non-hostile.

This assumption is met by:
those responsible for the TOE must ensure that the TOE is installed by administrators who will not attempt to subvert the security features, and operated in a manner that maintains IT security [OE.Benign, OE.Install].

9.1.1.8 A.Physical

The TOE is physically secure.

Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security [OE.Physical].

9.2 Security Requirements Rationale

This section provides evidence supporting the combining the internal consistency and completeness of the components (requirements) in the Security Target.

9.2.1 Security Functional Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target.

9.2.2 Objectives to Security Functional requirements

Table 9 - Mapping TOE Security Functional Requirements to Objectives

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FDP_IFC.2.	Complete information flow Control	FDP_IFC.1	FDP_IFF.1	O.HOST_INSTRUCTION
FDP_IFF.1	Simple security Attributes	None	FDP_IFC.1 FMT_MSA.3[4]	O.READ_ONLY O.WRITE_ONLY O.PHYSICAL_LEVEL_ENFORCEMENT
FPT_RVM.1	Non-Bypassability of the TSF	None	None	O.HOST_INSTRUCTION O.READ_ONLY O.WRITE_ONLY
FPT_SEP.1	TSF domain separation	None	None	O.PHYSICAL_LEVE_ENFORCEMENT

9.2.2.1 O.HOST_INSTRUCTION

The direction of the information flow through a Data Diode NIC cannot be altered by an instruction from a higher-level abstraction (e.g. operating system, application).

The objective is satisfied by requiring that the TSF enforce a unidirectional information flow SFP on all request from an external interface, including a host instruction passed to the device driver that is passed to the TOE across the PCI Bus, to move data packets through the Data Diode NIC [FDP_IFC.2]. To ensure there is no way to bypass this objective, the TSF ensures that TSP enforcement functions are invoked and succeed before each host request is serviced by the TSF (FPT_RVM.1)

9.2.2.2 O.READ_ONLY

A permanent condition exists whereby information that can be received by a Data Diode NIC installed on a host can be read by an executing abstraction attempting to read from that host connection, but an executing abstraction cannot write over the same connection.

[4] The management policy is purely environmental and its protection is purely physical (i.e., both outside the scope of the TOE and its SFPs). Once the TOE is installed into a host, no management action is necessary or possible.

This objective is satisfied by requiring that the TSF enforces a read-only unidirectional information flow SFP based on the physical transceiver configuration of the read-only Data Diode NIC. Also, the TSF explicitly permits a read-only information flow based on the fact that a receiving subject (host read or receive request) must be connected to a receive-only Data Diode that has been correctly physically modified such that it has a photodiode to receive light impulses, but no operational light source to send light impulses.[FDP_IFF.1]

To ensure there is no way to bypass this objective, the TSF ensures that TSP enforcement functions are invoked and succeed before any read request from the host is serviced by the TSF (FPT_RVM.1)

9.2.2.3 O.WRITE_ONLY

A permanent condition exists whereby information that can be sent by a Data Diode NIC installed on a Gateway can be written by an executing abstraction attempting to write to the Gateway connection, but an executing abstraction cannot read over the same connection.

This objective is satisfied by requiring that the TSF enforces a write-only unidirectional information flow SFP based on the physical transceiver configuration of the write-only Data Diode NIC. Also, the TSF explicitly permits a write-only information flow based on the fact that a sending subject (host write or send request) must be connected to a write-only Data Diode that has been correctly physically modified such that it has a light source to send light impulses but no operational photodiode to receive light impulses. [FDP_IFF.1]

To ensure there is no way to bypass this objective, the TSF ensures that TSP enforcement functions are invoked and succeed before any read request from the host is serviced by the TSF (FPT_RVM.1)

9.2.2.4 O.PHYSICAL_LEVEL_ENFORCEMENT

The TSP is enforced at the physical level and is unaware of higher-level abstractions.

This objective is satisfied by requiring that the TSF enforce a unidirectional information flow SFP based on the physical transceiver configuration of the Data Diode NIC. Also, the TSF explicitly permits the SFP based on the fact that a subject must be physically connected to the appropriate policy enforcement type of Data Diode that has been correctly physically modified such that it has only an operational light source to send light impulses or an operational photodiode to receive light impulses. [FDP_IFF.1]

To prevent tampering with the TSF from other devices, the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in that no untrusted subjects can perform physical modifications of the TSF and the TSP is maintained at the physical layer. This physical enforcement of the TSP is provided by separation of send and receive requests from subjects and that each request is an atomic action. [FPT_SEP.1]

9.2.3 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 9 lists each requirement from Section 6 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

Table 10 - Requirement Dependency Rationale

Functional Component	Dependency	Included
Complete information flow control (**FDP_IFC.2**)	FDP_IFF.1	FDP_IFF.1*
Simple security attributes (**FDP_IFF.1)**	FDP_IFC.1	FDP_IFC. 2
	FMT_MSA.3	NA
Non-bypassability of the TSP (**FPT_RVM.1**)	None	-
TSF domain separation (**FPT_SEP.1**)	None	-

Functional component FMT_MSA.3 is not applicable because the TOE enforces a fixed information policy that cannot be altered once the TOE is installed. Indeed the TOE cannot be modified after Owl completes initial assembly.

9.2.4 Security Functions to Security Functional requirements

This section maps the TOE security functional requirements to the TOE security functions and describes how each security functional requirement is met by a TOE security function.

Table 11 - Mapping SFRs to Security Functions

Security Function Security Funtional Requirements	INFORMATION FLOW	SELF-PROTECTION
FDP_IFC.2.	X	
FDP_IFF.1	X	X
FPT_RVM.1	X	
FPT_SEP.1		X

FDP_IFC.2 Complete Information Flow Control

The TSF enforce the unidirectional information flow SFP on any request from an external interface to move data packets through the TOE and all operations that cause that information to flow to and from subjects covered by the SFP.

If a host attempts to send traffic over a receive-only Data Diode NIC, buffers of data may be sent through the host device driver over the PCI Bus to the receive-only Data Diode NIC. The receive-only NIC will process the buffer, and convert binary to voltage, and voltage into light impulses. But when transceiver goes to transmit the light impulses, there is no light source since it has been physically disconnected. Also the send port has been physically blocked so that no light impulses can be transmitted. When the host does not receive a response from a connection request, it is up to the host protocol to deal with no response to the connection request. The TSF is maintained even though the host has attempted to send information through a receive-only Data Diode NIC.

If a host attempts to listen for traffic over a send-only Data Diode NIC, no signals/bits/buffers/voltage will be received by the device driver listening on the PCI Bus for data from the send-only Data-Diode NIC. The send-only Data Diode NIC has had the photodiode physically disconnected. Also the receive port has been physically blocked so that no light impulses can be received. When the host does not receive a response while listening for data from the send-only Data Diode NIC, it is up to the host protocol to deal with no data. The TSF is maintained even though the host has attempted to receive information through a send-only Data Diode NIC.

FDP_IFF.1 Simple security attributes

The TSF enforces the unidirectional information flow SFP based on the physical transceiver configuration of each Data Diode. A Data Diode NIC physically can only provide network traffic flow in one direction over any one-network connection and this TSP is enforced at the physical level. One send-only Data Diode NIC communicating with a receive-only Data Diode NIC is required for communication between them over the ports that they are exporting.

FPT_RVM.1 Non-Bypassability of the TSP

The TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. This is accomplished because the NIC card installed in a host is connected to a fiber-optic network. If the host is to receive information from the network a Receive-Only TOE NIC must be installed. There is no other way for information to be received from the fiber-optic network. If a host is to send to a fiber-optic network, then the Send-Only TOE NIC must be installed. There is no other way for information to be sent over the fiber-optic network.

FPT_SEP.1 TSF domain separation

The TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

The Data Diode NIC protects itself by not exporting an interface that can modify the TOE. The only interfaces exported are the PCI Bus interface and the network fiber optic interface. Neither interface can alter the TSF since the TOE has been physically modified to enforce the TSF and the TOE would have to be physically modified to violate the TSF. Since the TOE environment does not allow tampering with the host device in such a way that the Data Diode NIC can be removed by anyone other than an administrator, it is physically impossible to modify the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic.

9.2.5 Explicitly Stated Requirements Rationale

All requirements in this ST are reproduced relative to the requirements defined in CC v2.1, using the conventions described in Section 2.4.1.

In the context of CC v2.1 and International Interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements.

In the context of U.S. National interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements.

9.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package and is based on commercial development practices. This ST has been developed for a generalized environment with a low level of risk to the assets. The Security Objectives for the TOE were reviewed and EAL2 was found to be sufficient to address them.

9.4 Strength of Function Rationale

The TOE provides no IT security function for which a strength of function claim is appropriate. If a strength of function claim could be made, then an appropriate level would be SOF-basic since the assurance level for the TOE is determined to be EAL2.

9.5 TOE Summary Specification Rationale

Each subsection in Section 7, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.