National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Secure Switching Unit
Version D with Firmware Version 4.1

Report Number: CCEVS-VR-VID10253-2009
Dated: April 21, 2009
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 6757
Fort George G. Meade, MD 20755-6757

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the Secure Switching Unit Version D with Firmware Version 4.1, a product of DiCon Fiberoptics, Inc.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The TOE, the Secure Switching Unit (SSU), is an all-optical switch unit. All data flowing through the optical switches will be optical. Each switch has the capability to connect to optical fibers. These optical fibers are typically connected to optical transceivers on a computer or a signal processing/routing board on the other end. There is no requirement that the connection is to a host computer or a network. The SSU provides multiple point to point fiber connections.

The optical switches provide isolation between the output ports of the 1x3 switch block and between separate 1x3 switch blocks. There are 15 duplex pairs of 1x3 switches in the SSU. Two 1x3 switches make up a duplex 1x3 switch, so there are 30 actual switches in the SSU.

One way to think of the SSU is as an automated patch panel. Without the SSU, one would take an optical fiber and patch one optical port to another optical port (like the old telephone switchboards). The SSU provides a convenient way to switch ports with push buttons. However, unlike today's data/telecommunication routers, the SSU does not provide ANY sort of traffic or data packet management.

The SSU front LED panel provides switch position indicators. The front panel can be used to select the switch configuration modes, define user configurable modes[1], and to manually configure switch states. The console part on the back of the SSU can be used to define the programmable modes.

The evaluation of the SSU at EAL4, augmented with AVA_CCA.1 (Covert channel analysis) and AVA_VLA.3 (Moderately resistant), was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL) and the Common Criteria Evaluation and Validation Scheme (CCEVS). The information in this report is derived from the Evaluation Technical Report (ETR) prepared by the CygnaCom CCTL and the CCEVS (for AVA_CCA.1 and AVA_VLA.3).

The SSU was evaluated using the Common Criteria version 2.3 [CC] and the Common Methodology for Information Technology Security Evaluation, version 2.3 [CEM]. For the AVA_CCA.1 and AVA_VLA.3 assurance components, the CygnaCom CCTL used the methodology in CCEVS's *Methodology for Components above EAL4* guidance document. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

[1] A "mode" is a pre-stored channel configuration setting.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) CCEVS policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document DiCon Fiberoptics, Inc. Secure Switching Unit Version D Security Target, Version 0.10, 31 October 2008.

2 Identification

Target of Evaluation:	Secure Switching Unit Version D with firmware Version 4.1
Developer:	DiCon Fiberoptics, Inc. 1689 Regatta Blvd Richmond CA 94804
CCTL:	CygnaCom Solutions Suite 5400 7925 Jones Branch Drive McLean, VA 22102-3305
Evaluators:	Swapna Katikaneni, Cygnacom Solutions
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

3 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

3.1 Security Management

The SSU provides the ability perform the following management functions on the SSU:

- Define programmable modes using the Console port.
- Select switch configuration modes, define User Configurable Modes, and manually configure switch states using the Front Panel of the SSU
- Store and recall a preset mode (a pre-stored channel configuration for all 15 switches) via the Front Panel

The TOE allows for 16 total switch configuration modes, 9 are programmable modes. Administrators control the states of the switches using the front panel either by controlling individual duplex pairs or by recalling stored configuration modes.

3.2 Switching

Switching provides an optical connection between two ports by providing a low-loss path for a light beam to travel between two ports. The TOE provides all-optical switching using MEMS micro-mirrors in which the switching action is controlled by tilting the mirrors to redirect light beams. The mirror tilting mechanism is controlled electronically. This mechanism is proprietary. The signals are purely optical and the SSU does not alter, process, or store any information going through the optical fiber.

3.3 Protection of TOE Functions

Logical protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. In addition, the TOE provides a tamper evident seal and the ability to isolate ports from each other.

3.4 Isolation

The TOE provides the ability to isolate ports from each other to ensure that the security functions are executed on the correct port. Each of the 1x3 duplex pairs may connect the input port to only one output port (also referred to as channels) at a time.

Each of the 1x3 switches contains one optical On-off switch at each of the output ports. The 1x3 component provides optical isolation between the output ports by physical separation of output fibers. The On-off switch provides additional isolation by turning off (by optically cutting off the signal) the inactive output ports.

3.5 Tamper evident seal

All removable panels on the device will be protected by a tamper-evident seal. This tamper-evident seal will provide obvious signs of attempts to physically open the device.

3.6 SFR Summary

A summary of the SFRs for the TOE are included in the following table.

Table 1 TOE SFR Summary

TOE Security Functional Requirements (from CC Part 2)	
FDP_IFC.2	Complete Information Flow Control
FDP_IFF.1	Simple Security Attributes
FMT_SMF.1	Specification of Management Functions
FPT_PHP.1	Passive detection of physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
Explicitly Stated TOE Security Functional Requirements	
FPT_ISO_EXP.1	Optical Isolation

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL4 assurance requirements.

- ADO_DEL.2 Detection of modification
- ADO_IGS.1 Installation, generation, and start-up procedures
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

4.2 Environmental Assumptions

The TOE will be located in a location that provides physical security commensurate with the value of the optical data the TOE is switching, uninterruptible power, and the temperature control necessary for the reliable operation of the hardware. Only administrators will have physical access to the TOE.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL4 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. TOE depends on the environment for the Physical Protection of TOE.

The ST provides additional information on the assumptions made and the threats countered.

4.4 Architectural Information

The physical boundary of the TOE is the SSU device, including the SSU hardware Version D and SSU firmware Version 4.1. The hardware includes the chassis, front panel, motherboard, power back up, daughter board, user interface board, MEMS switch module. The firmware includes the backup power management, system firmware, main controller, power manager, and the user interface (UI) controller.

The key design specifications for the device are:

- Power: +28VDC
- Power Consumption: 50W maximum

- Back-up power hold-up time: 1 hour minimum
- Weight: 15 lbs. maximum
- Optical Crosstalk: -60dB maximum
- Startup Time: 30 seconds maximum

The PC or terminal directly connected to the SSU via the RS232 serial port is part of the IT environment. The optical fibers connected to the switches are also part of the IT environment.

The Secure Switching Unit (SSU) is an all-optical switch unit containing the following:

- 3U 19" rack-mount chassis
- 15 duplex pairs of 1x3 MEMS optical switches
- Front LED switch position indicators
- Unit status indicator (Ready, Fault, Power, and Backup LEDs)
- Built-In Self Test Capability
- Console Port used only to define Programmable Modes (via a direct serial connection to a PC or terminal – RS232) and cannot be used to control the switch. The console port is a DB-9 female connector implementing an RS232 interface on the back of the device.
- Front Panel to select switch configuration modes, define User Configurable Modes, and to manually configure switch states
- Electrical Power / Status Out Connector

There are 15 duplex pairs of 1x3 switches (30 actual switches) in the SSU. Two 1x3 switches make up a duplex 1x3 switch. This means that the two 1x3 switch (e.g. Switch 1 and Switch 2) will operate synchronously (e.g. they will both switch to port A (or B, C, or Default) at the same time. Each of the thirty actual switches can only connect 2 optical fibers at one time.

Each of the 1x3 switches provides a point to point optical connection, where the input port is connected to only one output port (also referred to as a channel) at a time. There are three possible output ports – A, B, and C. This means that at any given time, there is a maximum of 30 inputs (or fibers) connected to 30 outputs (or fibers). Since the data flows through the switch in the form of a light beam, the optical connection is bi-directional, that is it works the same in either direction. Thus the designation of inputs and outputs in the figure below is arbitrary, and the flow of light can either be from input to output, or from output to input. There is also a state in which the input port is not connected to any of the output ports. This state is called the "Default" state. After power up or "Reset", the SSU will go to the Default state.

The following diagram is a representation of a duplex pair consisting of two 1x3 switches, where each switch is composed of a 1x3 MEMS component (SW1 and SW5) and 3 On-Off MEMS components (SW2-4 and SW6-8). The SSU consists of 15 of the duplex pairs depicted below.

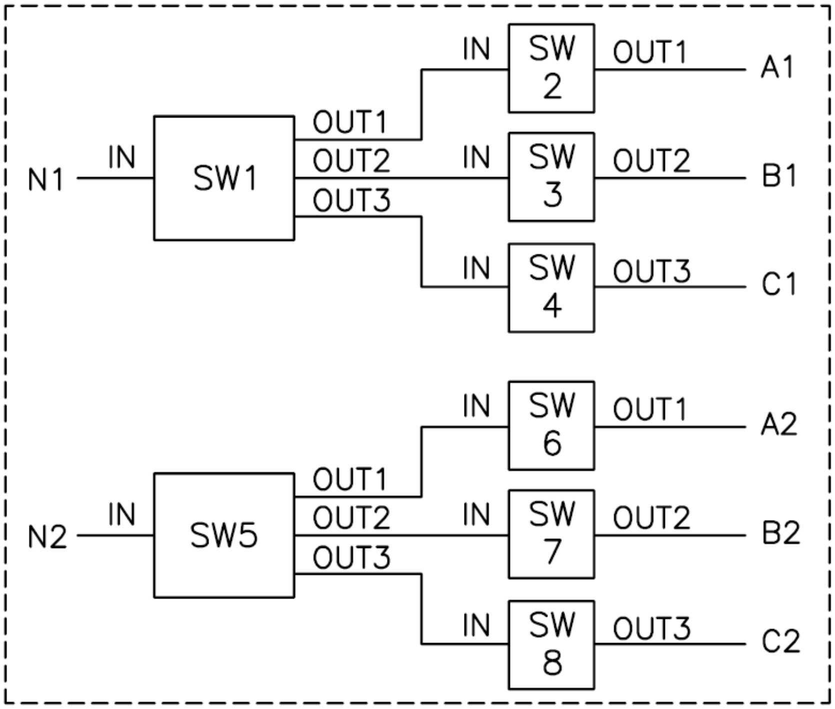

Figure 1 Duplex Pair

All input fibers (N1 to N30) are bundled into a common optical connector designated as INPUT N on the front panel. The output fibers A1 to A30, B1 to B30, C1 to C30, are also bundled into common optical connectors designated as CHANNEL A, CHANNEL B, CHANNEL C, respectively. The TOE has been tested using single wavelength, unmodulated 850nm test laser as the input.

The Electrical Power / Status Out connector provides grounding and power and serves as a fault indicator. The information conveyed by the status out pin is the same as the Fault LED, except when either the motherboard or user interface crashes in which case the one that did not crash signals a fault.

The SSU does not provide the ability to update the firmware without opening the SSU chassis. The chassis will contain a tamper evident seals to indicate any physical tampering.

The current channel for an individual switch is displayed on the LEDs on the front panel. To change the switch channels, the user pushes the pushbutton of the switch on the front panel. All switch control functions, except defining programmable modes, can only be accessed from the front panel.

There is no remote access allowed to the TOE other than the optical data which passes through the device unprocessed.

The TOE is transparent to the devices and the users of the devices on the other end of the optical fibers; these users are considered end users of the TOE.

5 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- DiCon Fiberoptics, Inc. Secure Switching Unit Version D with Firmware Version 4.1 Security Target, Version 0.10, October 31, 2008.
- Operation and Maintenance Manual Rev C4.

6 IT Product Testing

At EAL4, the overall purpose of the testing activity is “to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST” (14.9 [CEM]).

At EAL 4, the developer’s test evidence must include a test coverage analysis that shows that the “TSF has been tested against its functional specification in a systematic manner” (ATE_COV.2, Analysis of coverage [CC]). As a result, “All security functions and interfaces that are described in the functional specification have to be present in the test coverage analysis and mapped to tests in order for completeness to be claimed, although exhaustive specification testing of interfaces is not required.”(ATE_COV-2.4 [CEM]).

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset.

6.1 Developer Testing

The test approach consists of manual tests. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan & procedures do cover every possible combination of parameters for a given interface and every possible combination of parameters for a given security function. The test plan & procedures do stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The vendor’s testing purposefully intended to cover all the security functions as defined in Section 6 of the ST.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL4 evaluation.

6.2 Evaluator Independent Testing

The evaluation team performed the following activities during its on-site visit:

1. Installation of the TOE in its evaluation configuration (ADO_IGS.1)
2. Execution of a sample of the developer's functional tests (ATE_IND.2)
3. Independent Testing (ATE_IND.2)
4. Vulnerability Testing (AVA_VLA.2)
5. Configuration Management Audit (ACM_CAP.4)
6. Audit of Delivery Procedures (ADO_DEL.2)
7. Audit of Developmental Security Procedures (ALC_DVS.1)

The emphasis of CygnaCom's independent test is on areas where hostile intent would likely be expressed. Hence, the primary emphasis of the independent tests is on the input and the output ports and other external TSFI of the TOE.

CygnaCom has selected 100% of the tests DiCon provided as evaluation evidence. The tests were selected to exercise security functions described in the ST.

CygnaCom's independent tests augment and supplement the tests DiCon provided as evaluation evidence. Again, the emphasis is on the TSFI.

The penetration tests cover hypothesized vulnerabilities and potential misuse of guidance. The list hypothesized vulnerabilities was developed based on DiCon's vulnerability assessment and analysis of evaluation evidence. The tests for potential misuse of guidance cover installing the TOE from guidance documentation and sampling administrator procedures.

All tests passed. No further obvious vulnerabilities were found.

6.3 Moderately Resistant Vulnerability Analysis

Evaluation team testing at NSA was completed in April 2009. Using the results of the VLA.2 evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE in its evaluated configuration and conducted AVA_VLA.3 vulnerability testing. The NSA evaluation team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE was resistant to penetration attacks performed by attackers with moderate attack potential.

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

7 Test Configuration

7.1 Set-Up

Figure 2 shows the setup used for automated testing of the SSU. A Dicon Fiberoptics GP700 Fiberoptic System containing four 1x15 duplex switches will be used to automate switching of the test fibers. A PC is used to interface with the GP700 and the Power Meter for control and data acquisition through the GPIB bus. The laser source is split into 2 fibers using a 1x2 coupler. The 2 sources are then connected to the 2 inputs of the 1x15 duplex switch. This switch is then used to connect the laser source to any of the 15 duplex inputs of the SSU within the input connector. The output connectors of the SSU are likewise connected to 1x15 duplex switches. These are used to connect the outputs of the SSU to optical power meters.

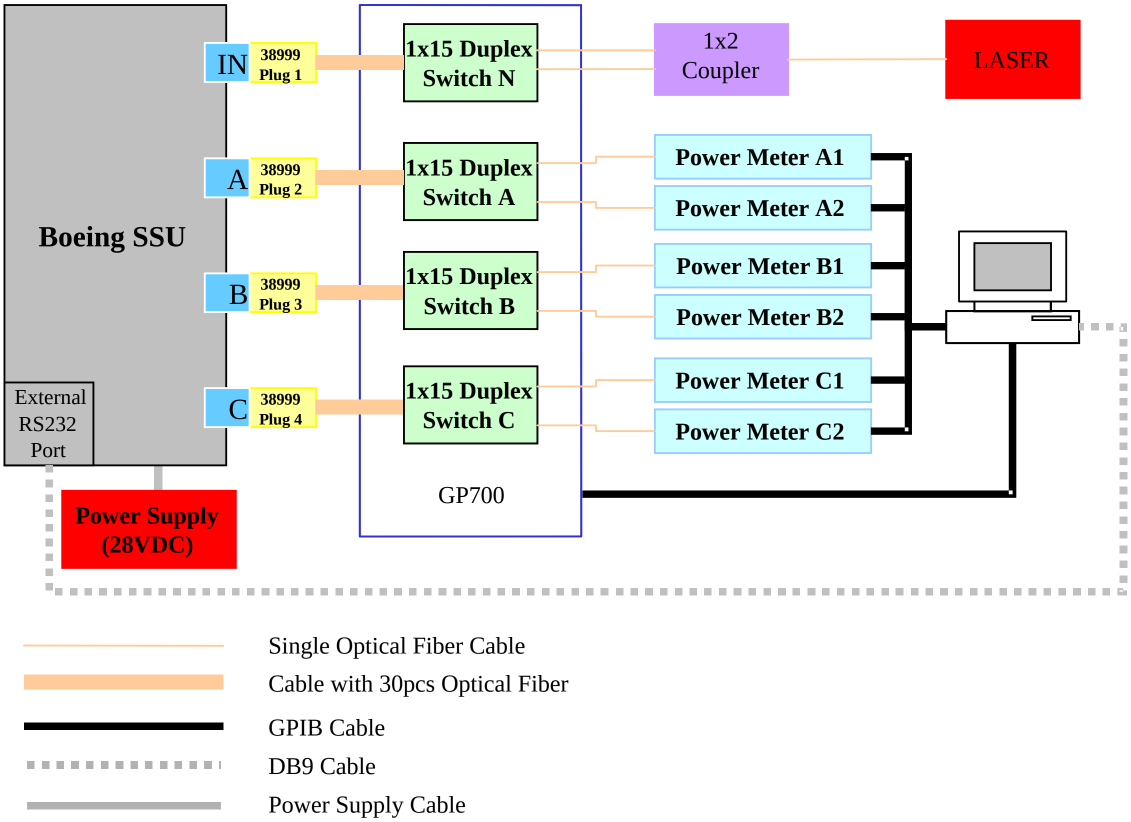

Figure 1 SSU Test Setup

7.2 Network Configuration

For testing purposes the SSU was connected to an 850nm laser. This laser is the same wavelength as the SSU is expected to be operated at. Since the SSU is an all-optical switch, it is data rate independent, and will function the same regardless of the data rate.

7.3 Test Software and Hardware

CygnaCom used common, open source tools whenever possible as well as the following tools that already available in the DiCon facility:

1. Proprietary tool developed using Labview for the GP700 which records the output power at all the channels while switching the input of the GP700.
2. Proprietary software program used to calibrate the daughter board

8 Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. Using the results of the VLA.2 evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE in its evaluated configuration and conducted AVA_VLA.3 vulnerability testing. The NSA evaluation team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE was resistant to penetration attacks performed by attackers with moderate attack potential. The TOE satisfies the EAL4 security assurance requirements, augmented with AVA_CCA.1 and AVA_VLA.3, as identified in Part 3 of the CC. The security assurance requirements are displayed in Table 2.

Table 2 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design

Assurance Component ID	Assurance Component Name
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.	Functional testing
ATE_IND.2	Independent testing - sample
AVA_CCA.1	Covert channel analysis
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.3	Moderately resistant

The overall evaluation result for the target of evaluation is Pass. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

The TOE is CC Part 2 Extended

The TOE is CC Part 3 conformant for EAL4 augmented with AVA_CCA.1 and AVA_VLA.3

9 Validator Comments/Recommendations

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL4 certificate rating be issued for the DiCon Fiberoptics, Inc. Secure Switching Unit Version D with Firmware Version 4.1.

10 Security Target

DiCon Fiberoptics, Inc. Secure Switching Unit Version D with Firmware Version 4.1 Security Target, Version 0.10, 31 October 2008. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

11 Glossary

The following table is a glossary of terms used within this evaluation.

All-optical switching	Switching in the optical domain, in which the switching action is obtained by redirecting light beams.
MEMS	Micro-electromechanical systems; a technology that embeds mechanical devices such as sensors, mirrors, actuators, and valves in semiconductor chips.
LED	Light emitting diode; a electronic device that lights up when electricity is passed through it.
SSU	Secure Switching Unit.

12 Bibliography

Uniform Resource Locators

Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

CygnaCom Solutions CCTL (http://www.cygnacom.com).

DiCon Fiberoptics, Inc. (http:// www.diconfiberoptics.com).

CCEVS Documents

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

Other Documents

[ST] DiCon Fiberoptics, Inc. Secure Switching Unit Version D with Firmware Version 4.1 Security Target, Version 0.10, 31 October 2008.