National Information Assurance Partnership

Cisco Optical Networking Solution

(ONS)

Validation Report

Report Number:	**CCEVS-VR-VID10561-2014**
Dated:	**12 September 2014**
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jandria S. Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Leidos Common Criteria Testing Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Optical Networking Solution (hereafter referenced as Cisco ONS). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of Cisco ONS was performed by Leidos formerly known as SAIC, in the United States and was completed in August 2014. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and scheme. The criteria against which the Cisco ONS TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation Versions 3.1, Revision 4.

The information in this report is largely derived from the ST, Evaluation Technical Report (ETR), the Assurance Activities Report (AAR) and associated test report. The ST was written by Cisco. The ETR, AAR and test report used in developing this validation report were written by Leidos. The product, when configured as specified in the installation guides, user guides, and ST satisfies all of the security functional requirements stated in the Cisco ONS Security Target, version 1.0 dated August 11, 2014 and the Protection Profile for Network Devices (NDPP).

The Cisco ONS TOE is the Multiservice Transport Platform (MSTP) that provides dense wavelength-division multiplexing (DWDM) and time-division multiplexing (TDM) solutions. The Optical Encryption Line Card provides the secure transport capability of the TOE. The card provides data confidentiality and data integrity over a fiber optic communication channel through the combination of cryptography and product architecture. The services include service transparency, flexible topology, completely reconfigurable traffic pattern, and simplified operations. The platform supports a variety of modules to enable wide deployment scenarios including access, metro, regional, and ultra-long-haul networks. The traditional transport services such as Ethernet and IP are also supported by the TOE. The TOE includes the hardware models as defined in Section 5.

A validation team from NIAP monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and verdicts of the ETR. The team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the product met all the security requirements and Assurance Activities contained in the NDPP. Therefore the team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Evaluation Methodology (CEM) for evaluations in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco Optical Networking Solution
Protection Profiles	U.S. Government Security Requirements for Network Devices (pp_nd_v1.1) version 1.1, 8 June 2012 Security Requirements for Network Devices, Errata #2, 13 January 2014
Security Target	*Cisco Optical Networking Solution Security Target*, Version 1.0, August 11, 2014
Dates of evaluation	January 2014 through August 2014
Evaluation Technical Report	*Proprietary Evaluation Technical Report for Cisco Optical Networking Solution Version 9.8.1.2*, Version 1.0, 25 July 2014
Assurance Activities Report	*Assurance Activities Report for Cisco Optical Networking Solution Version 9.8.1.2*, Version 2.0, 8 May 2014.
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R4, September 2012
Common Evaluation Methodology (CEM)	CEM version 3.1R4 dated September 2012and all applicable NIAP
Sponsor	Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
Developer	Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
Common Criteria Testing Lab	Leidos Common Criteria Testing Laboratory, 6841 Benjamin Franklin Drive, Columbia, MD 21046
Evaluators	Kevin Micciche and Greg Beaver
Validation Team	Jandria S. Alexander and Mike Allen of the Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None

International Interpretations

None

3 Security Policy

The security requirements enforced by the Cisco ONS were designed based on the following overarching security policies:

3.1 Audit

The Cisco Optical Networking Solution provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Optical Networking Solution generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. Auditing is always on to audit all events and therefore the administrator is only required to manage the audit data storage and archive of the log files. The TOE provides the administrator with a circular audit trail with a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are manually archived over a secure HTTPS/TLS connection to an external audit server.

3.2 Cryptographic Support

ONS is a FIPS validated product. The CAVP certificates are listed within the Security Target.

The TOE also provides cryptography in support of other Cisco ONS security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level.

The TOE provides HTTPS, as specified in RFC 2818, to provide a secure interactive interface for remote administrative functions and to support secure exchange of user authentication parameters during login. HTTPS uses TLS to securely establish the encrypted remote session. The TOE provides TLS 1.0, conformant to RFC 2246. The TOE only supports standard extensions, methods, and characteristics.

3.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

3.4 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters, password expiration as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection.

3.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS session or via a local console connection. The Cisco Transport Controller (CTC) is the only administrator interface permitted to manage the ONS in the evaluated configuration. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE; and
- Updates to the TOE.

Administrative users can be assigned one of the following security levels:

- Retrieve-Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance-Users can access only the ONS 15454 maintenance options.
- Provisioning-Users can access provisioning and maintenance options.
- Superuser-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. Superusers can also provision security policies on the TOE. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

3.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco ONS is not a general-purpose operating system and access to Cisco ONS memory space is restricted to only Cisco ONS functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

3.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also be configured to display an Authorized Administrator specified banner on the GUI management interface prior to accessing the TOE.

3.8 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over HTTPS and initiates secure HTTPS connections to transmit audit messages to remote syslog servers.

4 Assumptions and Clarification of Scope

All Threats to the TOE, Assumptions, and Organization Security Polices are consistent with those contained in: [NDPPv1.1].

.

4.1 Assumptions

The following assumptions were made during the evaluation of the Optical Networking Solution.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

- TOE Administrators are trusted to follow and apply all administrator guidance and maintain the TOE in its evaluated configuration.

  The TOE includes all the code that enforces the policies identified.

4.2 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 and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

The TOE claims exact compliance to the Protection Profile for Network Devices, Version 1.1, 08 June, 2012 and Security Requirements for Network Devices Errata #2, 13 January, 2014. Exact compliance indicates that the TOE implements the security functions exactly as specified by the PP; however, functions not described in the Security Target may be used, but were not tested as part of this evaluation.

The evaluation was conducted against the specific devices and software version as identified herein. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile, including any Errata, to which this evaluation claimed compliance.

Communications to and from the TOE is via a trusted path that is part of the environment and not part of this evaluation. Users must ensure the proper level of security is employed on this path.

The administrator is responsible for updating all patches and security updates.

The process to track flaws and updates may require purchase of a Service Level Agreement (See the Validator’s Comments, Section 10 below, for further details).

5 Architectural Information

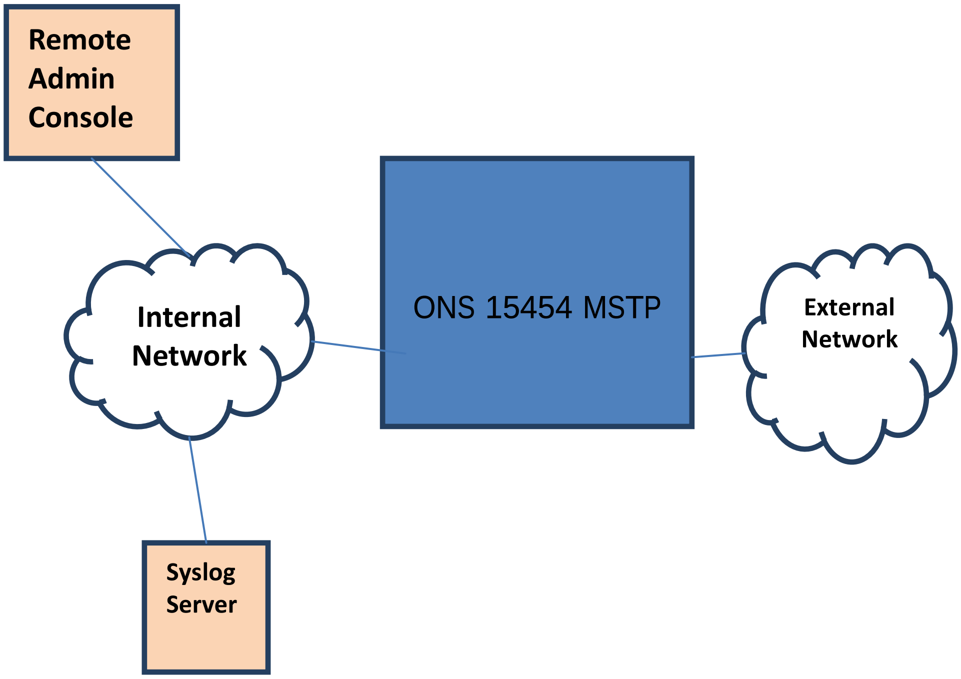
The TOE consists of one or more physical devices; the Optical Networking Solution (ONS) with Cisco IOS software. All of the ONS systems run the same version of the Universal Cisco Internet Operating System (IOS) software image Release 9.8.1.2 software which enforces the security functions being claimed regardless of the model.

The Cisco IOS configuration determines how packets are handled to and from the routers' network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the Optical Networking Solution (ONS) is to be remotely administered, then the management station must be connected to an internal network, HTTPS must be used to connect to the router. A syslog server can also be used to store audit records. A remote authentication server can also be used for centralized authentication. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

The following figure provides a visual depiction of an example TOE deployment.

Figure 1: TOE Deployment Example



5.1 Physical Boundaries

The TOE is a hardware and software solution that makes up the router models as follows: Cisco ONS 15454 M2 or ONS 15454 M6 DWDM.

The network on which they reside is considered part of the environment. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 9.8.1.2.

5.2 Hardware

The hardware is comprised of the following:

Cisco ONS 15454 M2, ONS 15454 M6 DWDM

Controller Card
15454-M-TNC-K9
15454-M-TSC-K9
15454-M-TNCE-K9
15454-M-TSCE-K9

Encryption Card
15454-M-WSE-K9

The network, on which they reside, is considered part of the environment. The software is comprised of the Universal Cisco IOS software image Release ONS 9.8.1.2.

The validated platforms consist of the following components:

Chassis (one or more):
15454-M2-SA
15454-M6-SA

Controller (Management) Cards (one or more):
15454-M-TNC-K9
15454-M-TSC-K9
15454-M-TNCE-K9
15454-M-TSCE-K9

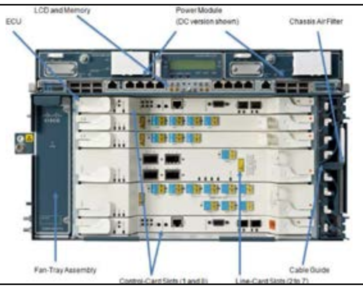
Encryption (Traffic Data) Card:
15454-M-WSE-K9

5.3 Software

ONS 9.8.1.2

5.4 Appliances

The TOE hardware includes the following appliances:

Hardware	Picture	Interoperability	Size	Power	Interfaces
Cisco ONS 15454 M2 Multiservice Transport Platform (with and without covers)	 	N/A	3.46 x 17.18 x 11.02 in.	100-240V	One slot for the control card and two slots for service cards. USB port,
Cisco ONS 15454 M6 Multiservice Transport Platform (with and without front cover)	 ECU LCD and Memory Power Module (DC version shown) Chassis Air Filter Fan-Tray Assembly Control-Card Slots (1 and 8) Line-Card Slots (2 to 7) Cable Guide	N/A	10.45 x 17.45 x 11.02 in.	100-240V	2 slots for redundant control cards and 6 slots for service cards.

5.5 Configurations

Permitted Configurations:

Chassis	Controller Cards	Encryption Card
15454-M2-SA	**Single** 15454-M-TNC-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TSC-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TNCE-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TSCE-K9	**Up to two (2)** 15454-M-WSE-K9
15454-M6-SA	**Single** 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9
	Single 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9
	Single 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Single 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9

Chassis	Controller Cards	Encryption Card
	Dual 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9

6 Documentation

Cisco offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The documentation for the TOE is:

Cisco Optical Networking Solution Common Criteria Configuration Guide
Cisco ONS 15454 DWDM Configuration Guide, Release 9.8
Cisco ONS 15454 Series Multiservice Transport Platforms
Cisco ONS 15454 Series Multiservice Transport Platforms Security Reference
Cisco ONS 15454 Series Multiservice Transport Platforms Connect the PC and Log into the GUI
Cisco IOS Command Reference

The security target used is:

Cisco Optical Networking Solution Security Target, 1.0, August 11, 2014.

7 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an NDPPv1.1.

Independent testing took place at the CCTL location in Columbia, Maryland in May 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in three distinct but representative configurations) in accordance with the provided guidance and exercised the Team Test Plan on equipment configured in the testing laboratory.

This effort involved installing and configuring the Cisco Optical Networking Solution components. Subsequently, the evaluators exercised all the tests cases. The tests were selected in order to ensure that each of the test assertions defined by the NDPPv1.1 were covered.

Also, the evaluators devised independent tests to ensure that start-up and shut down operations were audited, to verify the claimed methods of audit storage, to verify that administrator actions were audited, to verify that users are identified and authenticated, to verify use and restrictions of the management functions, to verify protected communication between the TOE and the trusted components of the operational environment, to verify trusted path and to verify protected update of the TOE software.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for NDPPv1.1 are fulfilled.

8 Evaluated Configuration

The TOE is the Cisco Optical Networking Solution installed and configured according to the Cisco Optical Networking Solution Common Criteria Configuration Guide as well as the Installation Guide for the respective Cisco Optical Networking Solution models included in the TOE.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, the NDPPv1.1, and the CCEVS.

The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Test Summary Report provided by the CCTL. 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 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Network Devices Protection Profile (NDPP). The evaluation determined the Cisco Optical Networking Solution TOE to be Part 2 extended, and meets the SARs contained the PP. All assurance activities and work units received a passing verdict.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Cisco Optical Networking Solution meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- Pay particular attention to the evaluated configuration of the devices as stated in the Security Target and Common Criteria Configuration Guide.
- NON-FIPS 140 mode of operation is excluded from the evaluation. This mode is to be disabled in the evaluated configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices version 1.1.
- The use of the local console for administration is specifically excluded from use once the device has been placed into the evaluated configuration.
- Please note that the evaluated functionality was scoped exclusively to the security functional requirements as specified in the Security Target. Any other functionality included in the product was not assessed as part of this evaluation.
- Note that certain network related functionality is excluded from the approved configuration and that some networking functions relative to the devices were not tested, nor can any claims be made relative to their security. The following features are not included in the evaluated configuration:
  - RS-232 local console
  - Telnet
  - FTP
  - HTTP
  - SNMP
  - SSH
  - SSL (pre-TLS)
- The following features and functions were not evaluated and should not be used in the evaluated configuration. No further conclusions can be drawn as to their effectiveness:
  - Synchronous Optical Networking (SONET)
  - Synchronous Digital Hierarchy (SDH)

- Synchronous Ethernet (SyncE)
- Reconfigurable Optical Add/Drop Multiplexers (ROADMs)
- Building Integrated Timing Supply (BITS)
- IEEE 1588v2 Precision Timing Protocol (PTP)
- OSI Layer 2 protocols such as CDP, VLAN protocols, Ethernet encapsulation protocols, etc.
- Routing protocols such as OSPF, BGP, etc.
- Protocol inspection engines (enabled with the “inspect” commands)

11 Security Target

Cisco Optical Networking Solution Security Target, Version 1.0, August 11, 2014.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DoD	Department of Defense
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

13 Bibliography

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

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R4, September 2012.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R4, September 2012.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R4, September 2012.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R4, September 2012.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R4, September 2012.
- Cisco Optical Networking Solution Security Target, Version 1.0, August 11, 2014
- Evaluation Technical Report For Cisco Optical Networking Solution, parts 1 and 2, version 1.0, July 21, 2014.
- Assurance Activities Report For Cisco Optical Networking Solution Version 9.8.1.2, Version 2.0, May 8, 2014.