National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

3e Technologies International

9715 Key West Avenue, 5th Floor

Rockville, MD 20850 USA

CyberFence 3e-636 Series Network Security Devices

Report Number:	**CCEVS-VR-10820-2017**
Dated:	**09/20/2017**
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

Paul Bicknell
Lisa Mitchell
MITRE Corporation

Ken Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Chris Keenan
Ed Morris
Catherine Sykes
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of 3eTI CyberFence 3e-636 Series Network Security Devices solution provided by 3e Technologies International. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in August 2017. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, as summarized in the publically available Assurance Activity Report, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015.

The Target of Evaluation (TOE) is the 3eTI CyberFence 3e-636 Series Network Security Devices.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team and provided guidance on technical issues. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the 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.

The technical information included in this report was obtained from the CyberFence 3e-636 Series Network Security Devices (NDcPP10) Security Target, version 0.7, September 19, 2017 and analysis performed by the Validation Team.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	3eTI CyberFence 3e-636 Series Network Security Devices (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015
ST	CyberFence 3e-636 Series Network Security Devices (NDcPP10) Security Target, version 0.7, September 19, 2017
Evaluation Technical Report	Evaluation Technical Report for CyberFence 3e-636 Series Network Security Devices, version 0.3, September 12, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	3e Technologies International
Developer	3e Technologies International
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Paul Bicknell, MITRE Corporation
	Lisa Mitchell, MITRE Corporation
	Ken Stutterheim, The Aerospace Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is CyberFence 3e-636 Series Network Security Devices. 3eTI's 636 Series Network Security Devices offer the multiple capabilities necessary for protecting embedded devices and safety-critical industrial control systems (ICS) against internal and external attacks. The core capabilities include: network access control, OSI Layer 2 and Layer 3 packet filtering, industrial control protocols packet inspection and secured application data transportation (via encryption).

The TOE is composed of both hardware and firmware. All four models of the 3e-636 series devices share the identical hardware. The 3e-636L3 was evaluated with version 5.1.300. The evaluated firmware version for 3e-636L2, 3e-636H and 3e-636A is version 5.1.300 with variant product features enabled or disabled based on EEPROM entries created at manufacturing time for that specific model. The sets of firmware share the same OpenSSL library and kernel drivers and have the identical software modules that implement the CPP_ND SFRs such as IPsec and TLS server.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

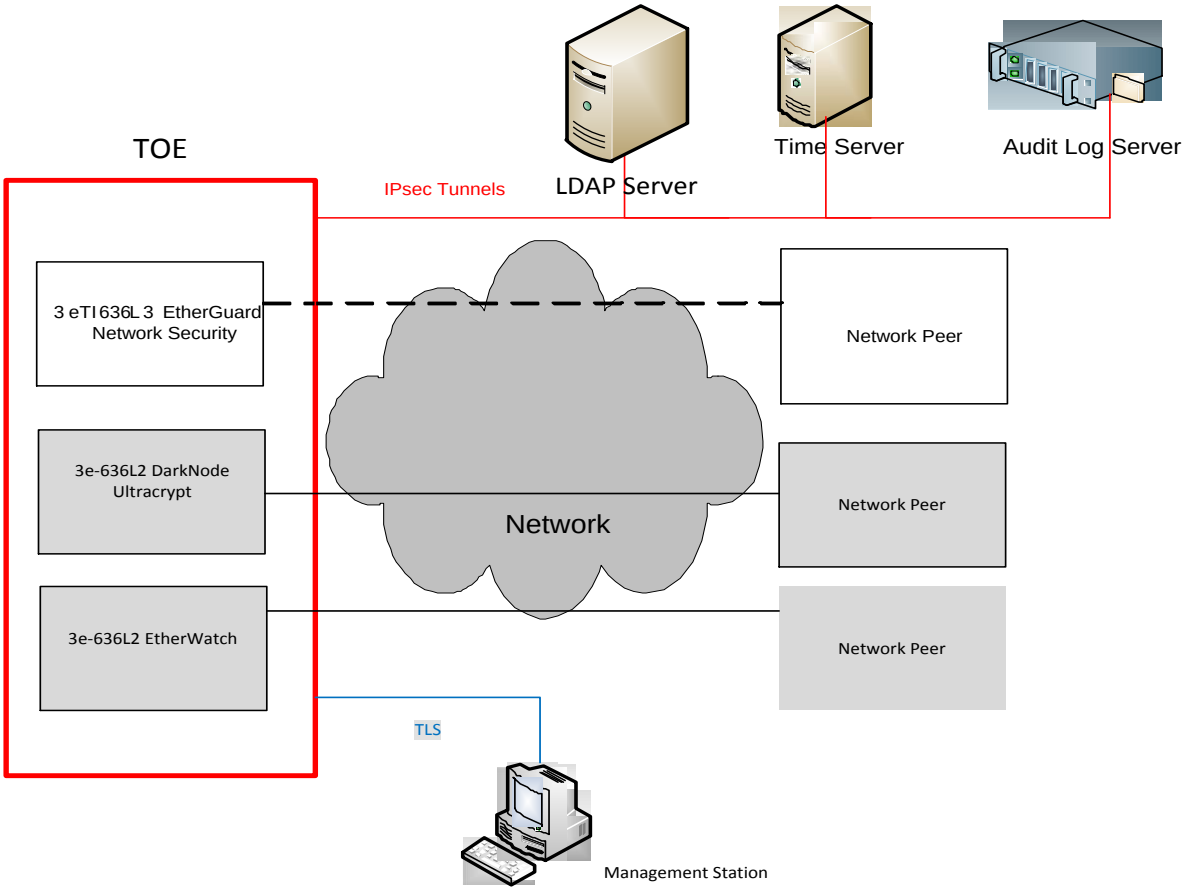
Device Name	**Included Device Product Features**			
	VPN Encryption	**VLAN Encryption**	**Access Control**	**Industrial Protocol Packet Inspection**
3e-636L3 EtherGuard	X		X	X
3e-636L2 Darknode		X	X	X
3e-636H Ultracrypt		X		
3e-636A EtherWatch			X	X

The TOE requires the following Operational Environment support which is not included in the TOE's physical boundary.

- **Administrator Workstations:** Trusted administrators access the TOE through the TLS/HTTPS protocol.
- **Audit Servers:** The TOE relies upon the audit server for storage of audit records. The TOE itself stores limited amount of the audit records in its internal persistence storage. Those audit records are accessible and exportable through the Web GUI interface.
- **NTP Servers:** The TOE relies upon an NTP server to provide reliable time**.** If the time is configured locally, the TOE will use its own reliable hardware clock to maintain time as well.
- **LDAP Server:** The TOE relies on the LDAP server for centralized authentication of administrator if the security administrator chooses this configuration. The TOE can also authenticate administrator using local user name and password.

3.2 TOE Architecture

The figure below illustrates the typical deployment use case and operational environment for TOE devices.



All devices operate in the same operational environment. IPsec tunnels are used to secure the communication between the device and external servers such as NTP server, Audit log server and LDAP server. All devices offer the same HTTPS/TLS based GUI interface for device configuration and management.

3.3 Physical Boundaries

The TOE physical boundary defines all hardware and firmware that is required to support the TOE's logical boundary and the TOE's security functions. The TOE hardware platform uses FreeScale MPC8378E CPU and the TOE's firmware contains an embedded Linux Kernel customized by 3eTI based on kernel version 4.6. In short, the TOE's physical boundary is the physical device for all models.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE generates auditable events for actions on the TOE and is capable of selective audit record generation. The records of those events can be viewed within the TOE Management Interface or they can be exported to audit systems in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. Additionally, all administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

4.2 Cryptographic support

The TOE uses NIST SP 800-90 DRBG random bits generator and the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC to secure the trusted channel and trusted path communication. The TOE is designed to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification of those secrets.

4.3 Identification and authentication

The TOE provides Identification and Authentication security functionality to ensure that authorized users are properly identified and authenticated before accessing TOE functionality. The TOE enforces a password-based authentication mechanism to perform administrative user authentication. Passwords are obscured while being entered during any attempted login. Administrative users can be authenticated via either local user database or remote LDAP server. The TOE also authenticates its IPsec peers; the authentication is performed over IKEv2 SA phase of mutual authentication between IPsec peers.

4.4 Security management

The Web Management Application of the TOE provides the capabilities for configuration and administration. The Web Management Application can be accessed via the dedicated local Ethernet port configured for "out-of-band" management. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

An authorized administrator has the ability to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized administrator the capability to manage how security functions behave. For example an administrator can enable/disable certain audit functions query and set encryption/decryption algorithms used for network packets.

4.5 Protection of the TSF

Internal testing of the TOE hardware and software ensures that all security functions are running and available before the TOE accepts any communications. The TSF prevents reading of pre-shared keys, symmetric keys, private keys, and passwords. The TOE uses electronic signature verification before any firmware/software updates are installed to defend against tampering.

4.6 TOE access

The TOE provides the following TOE Access functionality:

- TSF-initiated session termination when a connection (remote or local) is idle for a configurable time period
- Administrative termination of own session
- TOE Access Banners

4.7 Trusted path/channels

The TOE uses TLS/HTTPS for integrity and disclosure protection of administrative session communications.

The TOE uses IPsec to protect communication with network entities, such as a log server, NTP server and LDAP server. This prevents unintended disclosure or modification of logs and management information.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015

That information has not been reproduced here and the NDcPP10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP10 and supporting technical documentation as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and the Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, dated February 27, 2015 as performed by the evaluation team). All NIAP Technical Decisions related to the protection profile security functional requirements were considered and applied as necessary.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- 636 Series User Guide, Revision F, August 24, 2017

Please note that any other documentation delivered with the product or that may be accessible on-line that is not listed above was not included in the scope of the evaluation nor was it used to set the product into its evaluated configuration, and therefore should not be relied upon to place the device into the compliant configuration.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report (NDcPP10) for CyberFence 3e-636 Series Network Security Devices, Version 0.4, September 12, 2017 (DTR).

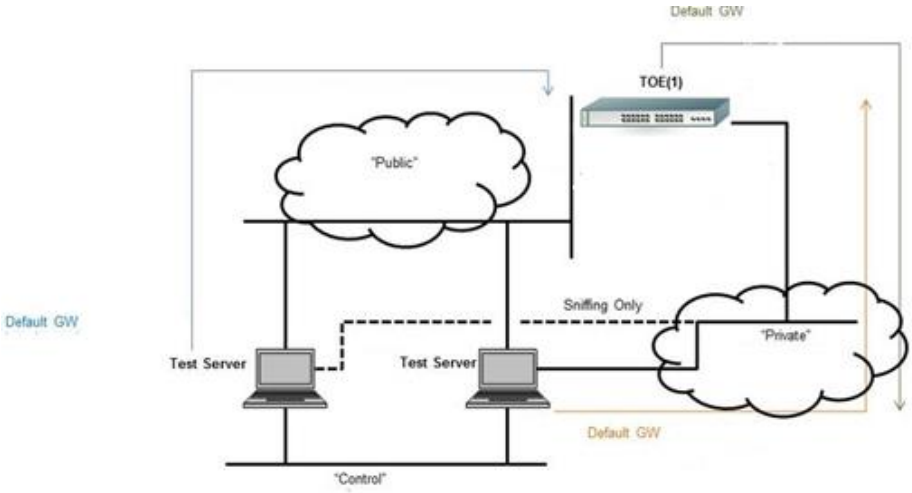
8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP10 including the tests associated with optional requirements.

Test Environment



9 Evaluated Configuration

The evaluated configuration consists of the following models and the 3eTI user guide documentation as noted above.

- 3e-636L3 EtherGuard
- 3e-636L2 Darknode
- 3e-636H Ultracrypt
- 3e-636A EtherWatch

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the

CyberFence 3e-636 Series Network Security Devices TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP10.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the CyberFence 3e-636 Series Network Security Devices that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP10 related to the examination of the information contained in the TSS.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP10 and recorded the results in a Test Report; summarized in the AAR.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "ultra electronics", "3eti", "darknode", "etherwatch", "etherguard", "ultracrypt", "3e-636L3", "3e-636L2", "3e-636H", "3e-636A", "mpc8378e", "openssl 1.0.2". Based on the results, no vulnerabilities existed in the TOE at the time of the evaluation that were exploitable.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed above to ensure the evaluated configuration is established and maintained.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include security based functional features such as VPN and VLAN encryption or industrial protocol packet inspection, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated version of the products utilizes firmware version 5.1.300 and no earlier or later versions were evaluated and therefore cannot be considered as compliant.

The TOE stores a limited amount of audit records in its internal persistent storage. It is recommended that the administrator configure the TOE to export audit logs to a remote audit storage server.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *CyberFence 3e-636 Series Network Security Devices (NDcPP10) Security Target, Version 0.7, September 19, 2017*.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is

complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015

[5] Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, dated February 27, 2015

[6] CyberFence 3e-636 Series Network Security Devices (NDcPP10) Security Target, Version 0.7, September 19, 2017 (ST)

[7] Assurance Activity Report (NDcPP10) for CyberFence 3e-636 Series Network Security Devices, Version 0.5, September 19, 2017 (AAR)

[8] Detailed Test Report (NDcPP10) for CyberFence 3e-636 Series Network Security Devices, Version 0.4, September 12, 2017 (DTR) <Evaluation Sensitive>

[9] Evaluation Technical Report for CyberFence 3e-636 Series Network Security Devices, Version 0.3, September 12, 2017 (ETR)

[10] Ultra Electronics 3ETI 636-Series User's Guide, Rev F, August 24, 2017