Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : STQC/CC/1415/14/CR

Product / system : Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10 EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35)

Dated: 16th April, 2017

Version: 1.0

Government of India
Ministry of Communication & Information Technology
Department of Electronics and Information Technology
Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi – 110003
India

Product developer:	ECI Telecom India Pvt Ltd
TOE evaluation sponsored by:	ECI Telecom India Pvt Ltd
Evaluation facility:	ERTL(E)-CCTL, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	Subhendu Das, Malabika Ghose & Debasis Jana
Evaluation report:	STQC IT (KOL)/STQC/CC/1415/14/ETRv1.0
Validation Personnel:	Alok Sain

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	ECI Telecom India Pvt Ltd
Developer	ECI Telecom India Pvt Ltd
The Target of Evaluation (TOE)	Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10 EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35)
Security Target	Security Target identification: ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Security Target
Brief description of product	The TOE consists of LightSoft and EMS-APT software executing on one or more dedicated Solaris servers, the LightSoft client-side application executing on Solaris or Linux workstations, and the NPT-1010, NPT-1020, and NPT-1200 software executing on supported appliances. It is a Network Management System (NMS) providing the control and monitoring of all products of the developer deployed by any service provider. The TOE components communicate with one another via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network from other (non-TOE) devices. The NPT Software processes all inputs on User Interfaces as user input for forwarding only. No other functionality is available through these interfaces.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	16th April,2017

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification

scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/DeitY/MCIT/Govt. of India);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

ECI Telecom India Pvt Ltd is the developer and sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on 16th Aug 2016 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [ERTL (E)-CCTL], ERTL (EAST), Block-DN Sector-V, Kolkata. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of LightSoft and EMS-APT software executing on one or more dedicated Solaris servers, (optionally) the LightSoft client-side application executing on Solaris or Linux workstations, and the NPT-1010, NPT-1020, and NPT-1200 software executing on supported appliances. The dependencies for each of the components are described in subsequent paragraphs.

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/1415/14 dated 19th March 2015.
The TOE as described in the [ST] is called as LightSoft. It is a Network Management System (NMS) providing the control and monitoring of all ECI products deployed by any service provider. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and ERTL (E)-CCTL, Kolkata Operating Procedure OP-07.
The evaluation has been carried out under written agreement [dated July 2015] between ERTL (E)-CCTL, Kolkata and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B 2 Identification of TOE

The TOE is the Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10 EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35).

The specific devices are identified as hardware / software/ firmware requirements of TOE:

Table 1: Requirements for LightSoft / EMS-APT server

Item	Requirements
Base Hardware	7 virtual CPUs
Memory	64 GB
Hard Disk	85 GB
Operating System	Hardened Solaris x86 11.2 Rev01
Desktop	CDE 5.10, X11 Version 1.0.3
CORBA	Orbix 6.3.6 with fix OR0301-01

Table 2: Requirements for LightSoft Client side application

Item	Requirements
Base Hardware	5 virtual CPUs
Memory	1 GB
Hard Disk	2 GB
Operating System	Solaris x86 11.2 Rev01
CORBA	Orbix 6.3.6 (installed during client-side application installation)

B 3 Security policy

There are following organizational security policies that the TOE must meet.

Table 3: Organizational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of activities.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 4: Assumptions

A.Type	Description
A.ECI	Administrators perform installation of the TOE in conjunction with ECI personnel.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits traffic from entering the management network.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

B.5 Evaluated configuration

The TOE consists of LightSoft and EMS-APT software executing on one or more dedicated Solaris servers, (optionally) the LightSoft client-side application executing on Solaris or Linux workstations, and the NPT-1010, NPT-1020, and NPT-1200 software executing on supported appliances. The dependencies for each of the components are described in subsequent paragraphs.

The Solaris server that hosts the server side of the LightSoft NMS and EMS-APT software components of the TOE is supplied by ECI. The following table provides details of the server as supplied. The Oracle DB is in a dedicated zone on the Solaris server.

The client-side application of LightSoft can be installed on the same system as the server component (in a separate zone) and be accessed remotely by users. The client-side application also may execute on Solaris, Solaris X86 or Linux workstations. In this mode the application establishes remote CORBA connections to the server. The following table provides minimum requirements for workstations hosting the client-side application.

The NEs managed by LightSoft/EMS-APT may be any combination of the NPT-1010, NPT-1020, and NPT-1200.

The TOE components communicate with one another via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network from other (non-TOE) devices.

Each of the NPT appliances provides a dedicated network interface for management interactions. The management interface must be connected to the segregated management network.

Table 5: Details of evaluated instantiations of the TOE

The image files	File size in bytes	Hash values of the image files	Hardware platform	Software Version and Release
OSC-P11.2.12_x86-91949.iso GLOBAL ZONE	713,711,616 bytes	MD5: 366dfb8ec5711220a9a6c5f5e3e7c25c / SHA2: 9F712A767CC8E4DCF7E761793487DB92B48D6EA4DEE6F61A8F4C131EC8376743	Solaris Information: Version: 5.11 Rev. 11.2 Initial Installation Media: Sol_P11.2_Rev01	Version 11.2
OraSrv-11.352.iso ORACLE ZONE	3,63,70,83,725 bytes	MD5: 99D78685DBCCB818F2506A05D8FFAA2A / SHA2: FC80E9E4EBB343EB2B343F38D2D0EF099108292217BDE7C83A69766D89195CD9	Solaris Information: Version: 5.11 Rev. 11.2 Initial Installation Media: Sol_P11.2_Rev01	Version 11.352
NMSsrv_V11.2_R1.1120.04113-X91899.iso NMS SERVER	4,38,67,66,848 bytes	MD5: 161F5F85A35EFEAEE5FAB40BBD522D6D /SHA2: 14EC8A3FF8FCBD563743A6A8BCCF202D4942CED4929A45A5D265465F90253F85	Solaris Information: Version: 5.11 Rev. 11.2 Initial Installation Media: Sol_P11.2_Rev01	Version 11.2
emsbgf_sol_x86_4.0.20.iso EMS-APT ZONE	1,55,54,41,664 bytes	MD5: 523E277B223A80D19773DC9486BBA3C2 / SHA2: 63BA78FF071AAC1FEA57630F48AC097FB08DA49C308F91AF60485E4422E8028D	Solaris Information: Version: 5.11 Rev. 11.2 Initial Installation Media: Sol_P11.2_Rev01	Version 4.0.20 Release
NMScli_V11.2_R1.1120.04113.iso NMS CLIENT ZONE	71,37,11,616 bytes	MD5: 945e27876b1453244847cfcc0041c531 / SHA2: E183D7201ECFB885717ED70A0EA7D6C7381DE94E24661B014ADB7586088CC46C	Solaris Information: Version: 5.11 Rev. 11.2 Initial Installation Media: Sol_P11.2_Rev01	Version 11.2
NPT1010_Emb_4035.bin NPT1010	1,60,92,192 bytes	MD5: cc65b46c4d4936e116b8fbaf46d134be / SHA2: 7883046C2376D925AD5F27FE7F9716D8C5C0CAEB5A08D119BC440C0EC721E054	NPT 1010	Version 4.0.35
NPT1020_Emb_4035.bin NPT 1020	6,75,59,456 bytes	MD5: a1a24ab1d3bf32fa8f0592118494e146 / SHA2: BE62B2BC09E0D66A050D1CF2E328D1C0F4071ABB3B0D90EE3DF832877AC1FC67	NPT 1020	Version 4.0.35
NPT1200_Emb_4035.bin NPT 1200	9,57,83,968 bytes	MD5: 26ec90eceb43886a70f82c1c34fc1451 / SHA2: 49C604243375EF9B2D2A8FEDCA57F95EAA475DFBE0E2F6E0F99ABDDDC59C0929	NPT 1200	Version 4.0.35

B.6 Document evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Security Target.
2. **TOE Architecture/Functional Specification and Design description**: ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Development Document.

3. **Preparative procedures**:.ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Common Criteria Supplement
4. **Configuration Management, Capability /scope and TOE delivery**:.ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Configuration Management Plan
5. **Test cases, logs and coverage**: ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Test Plan and Procedures, Version 1.2.

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the only subsystem of the TOE (i.e. router subsystem) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization of the TOE and also means of protection of the TOE from tampering and bypassing.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were also clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences were found to comply with the requirements of CCv3.1 for EAL2.

B 7 Product Testing

Testing at EAL2 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analyzed the developer's test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.

The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document.

The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results.

While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

a. Security Audit

The TOE is capable of generating audit records. The LightSoft and EMS-APT servers generate audit records for actions taken by their users and maintain a separate audit trail. The audit trail consists of Security Logs and Activity/Action Logs; audit records for startup of the audit function are stored in the NMSGF.log file in the /sdh_home/nms/logs directory.

The client-side GUI application provide authorized users with the LightSoft Role of Admin or Security Administrator View Activity Log or View Security Log capability with the ability to review audit records in a human readable form in LightSoft. Users with the EMS Role of Admin or Security Admin may review audit records in a human readable form in LightSoft. Users that do not have those capabilities or roles do not have access to any audit record information.

b. User data protection

ACLs may be configured for Ethernet ports of the NPTs. Each ACL specifies a list of source and destination MAC addresses that may be permitted or denied through the interface. If the flow is permitted, received packets are forwarded; if denied, received packets are silently dropped. If no ACL is associated with a port, all packets are forwarded.

c. Identification and authentication

The TOE requires all users of the client-side GUI application to successfully identify and authenticate themselves before access is granted to any TSF data or functions. User credentials are collected via the GUI and validated by the TOE. When a password is supplied, the TOE echoes a single dot for each supplied character to obscure the user input. If an invalid password is supplied, the count of unsuccessful login attempts for the User Account is incremented. If the supplied password is valid, the count is reset to 0.

Consecutive login failures for each defined user account are tracked. If the administrator configured number of consecutive failures is met for a user account, that user account is automatically locked. After an administrator configured number of minutes, the account is automatically unlocked. Administrators may manually unlock the account as well.

d. Security management

The GUI of TOE grants access to TSF data according to the Roles. Access is further limited by the Resource Domains associated with the User Account. Access to TSF data other than that specified in the table is prevented.

B 7.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities from public domain, scanning tools are used. Scanning was conducted to find out open ports and their vulnerabilities. OpenVas scanning tool is used with the latest feeds to find out hypothesized potential vulnerabilities present in the TOE.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analyzed to find out potential security vulnerability and the same is listed in.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The potential vulnerabilities with higher than 'Basic' attack potential are treated as residual vulnerabilities.

Penetration testing scenarios are summarized as below:

- TSF behavior in case of flooding with TCP malformed packets on EMS-APT server.
- TSF behavior in case of flooding with TCP malformed packets on Global Zone.
- TSF behavior in case of flooding with TCP malformed packets on Oracle zone.
- TSF behavior in case of flooding with TCP malformed packets on NMS server.
- TSF behavior in case of flooding with TCP malformed packets on NMS client.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

The TOE was evaluated through evaluation of its documentation, virtual site visit, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07].

Documentation evaluation results:

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CCv3.1 for EAL2.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that 'Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10 EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35)' behaves as specified in its

[ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

B 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that 'Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10 EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35)', satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification**.

However it should be noted that there are no **Protection Profile** compliance claims.

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function
TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Security Target
6. [ETR]: Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/1415/14/ETR v 1.0
7. [OP-07]: CCTL operating procedure