



Designation Requirements for Telecom Security Testing Laboratories

Doc. No.: **NCCS/SLR/03**

All Rights Reserved and no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without written permission from the
Department of Telecommunications, New Delhi

National Centre for Communication Security
Department of Telecommunications, Ministry of Communications
2nd Floor, City Telephone Exchange
Sampangirama Nagar, Bangalore -560027.

Amendment Record

Sl.No	Date	Issue	Details of change

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 2 of 12

CONTENTS

1.0 Scope of Document	4
2.0 General Information	4
2.1 Terms and definitions.....	4
2.2 References	5
3.0. Designation Criteria	6
4.0 Scheme Specific Requirements.....	6
4.1 Specific Requirements	6
4.1.4 DUT Evaluation requirements	9
4.1.5 Operational requirements and obligations	10
4.2 Evaluation activities of TSTL	11

1.0 Scope of Document

1.1 The Indian Telegraph Rules, 1951, PART XI, Testing & Certification of Telegraph, (Rule 528 to 537) provides that every Telecom equipment must undergo prior mandatory testing and certification.

1.2 In this context, Department of Telecommunications has come out with a “Communication Security Certification Scheme (ComSeC)” vide document No. NCCS/ComSeC/01/01102019 for Security Certification of Telecom equipment.

1.3. The general criteria for laboratory approval are laid down in the international standard ‘General Requirements for the competence of testing and calibration laboratories (latest version of ISO/IEC 17025)’and Telecom Security Testing Laboratories (TSTL) seeking designation must meet all of these requirements.

1.4. This document provides scheme specific requirements for performing conformity assessment against Security Requirements for Telecom equipment prescribed by the Department of Telecommunications (DoT). These are considered to be minimum requirements for TSTLs being designated against DoT’s TSTL Designation Scheme (Refer to “Procedure for designating Telecom Security Testing Laboratories – Doc. No NCCS/SLR/01”).

1.5 Security requirements for Telecom equipment are published equipment wise and/or for a group of Telecom equipment by DoT in the form of Indian Telecom Security Assurance Requirements (ITSAR) which are available online.

2.0 General Information

2.1 Terms and definitions

2.1.1. **Certification Body (CB)** means a body that issues a conformance certificate and may also conduct conformity assessment activities. Security Certification Division of NCCS entrusted with the function of Certification of Telecom equipment will be the Certification Body.

2.1.2. **Client** means indigenous Original Equipment Manufacturer (OEM) or Local Representative (LR) of foreign OEM or Importer who has chosen to test his Telecom equipment by a Designated TSTL through DoT’s testing and certification process

2.1.3. **Designation** means the authorisation given by Security Lab Recognition (SLR) Division of NCCS to a Telecom Security Testing Laboratory (TSTL) to undertake specified conformity assessment activities.

2.1.4. **Designated TSTL** means a Telecom Security Testing Laboratory designated by Designating Authority.

2.1.5. **Designating Authority (DA)** means Security Lab Recognition (SLR) Division of NCCS with the authority to designate, monitor, suspend or withdraw designation of TSTLs to conduct conformity assessment activities within its jurisdiction..

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 4 of 12

- 2.1.6. **DoT** means the Department of Telecommunications with its headquarters at Sanchar Bhavan, 20, Ashoka road, New Delhi- 110001
- 2.1.7. **DUT** refers to the Device Under Test.
- 2.1.8. **ITSAR** means Indian Telecom Security Assurance Requirements. ITSAR is published by Security Assurance Standards (SAS) Division of NCCS for a Telecom equipment or a group of Telecom equipment and gives the list of Security Requirements that a Telecom equipment or a group of Telecom equipment must comply with.
- 2.1.9. **NABL** stands for National Accreditation Board for Testing and Calibration Laboratories, New Delhi, India.
- 2.1.10. **National Centre for Communication Security (NCCS)** refers to a centre of DoT that is vested with the responsibility of developing Security standards/ requirements and activities associated with the security testing and certification of Telecom equipment
- 2.1.11. **Security Requirements** means set of parameters/standards/ requirements/ specifications etc. specified by DoT with regard to security to be complied by Telecom equipment. DoT publishes Security Requirements for Telecom equipment or a group of Telecom equipment in the form of document called ITSAR.
- 2.1.12. **Telecommunication equipment** also referred to as ‘Telecom equipment’ is synonymous with ‘Telegraph’, as defined in Section 3 of Indian Telegraph Act, 1885, and the terms are interchangeable.
- 2.1.13. **Telecom Security Testing Laboratory (TSTL)** refers to a Telecom Test Laboratory having the capability to test Telecom equipment for conformance to ITSAR.
- 2.1.14. **Validator** is an authorised representative of the Certification Body who is responsible for technical oversight of the evaluation process in a TSTL

2.2 References

- 2.2.1 Latest version of ISO/IEC 17025 General Requirements for the Competence of Testing and Calibration Laboratories
- 2.2.2 Latest version of Procedure for Designating Telecom Security Testing Laboratories– Doc. No NCCS/SLR/01
- 2.2.3 Latest version of Indian Telecom Security Assurance Requirements (ITSARs) published by NCCS
- 2.2.4 Latest version of Procedure for Security Certification of Telecom Equipment – Doc.No. NCCS/SC/01

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 5 of 12

3.0. Designation Criteria

3.0.1 All TSTLs seeking Designation for conducting Security Testing of Telecom equipment against ITSAR requirements must comply with the following mandatory requirements:

- a) Accreditation by any recognised Indian accreditation Body like NABL, in accordance with latest version of ISO/IEC 17025 for the discipline - Software and IT system covering Application Security Testing (OWASP,CWE 25), Vulnerability Analysis & Non-destructive Penetration Testing (CIS; NIST SP 800-115.)
- b) Scheme specific requirements for performing conformity assessment of Telecom equipment against ITSAR requirements

4.0 Scheme Specific Requirements

This section describes the scheme specific requirements that a TSTL must meet. These requirements are subdivided into the following categories:

4.1 Specific Requirements

- a) **Conflict of interest requirements** which are concerned with the degree of organizational separation within the TSTL, to ensure that all ITSAR evaluation work is performed in an objective manner, without undue influence from within the facility.
- b) **Facility requirements** which are concerned with a TSTL's physical and IT/Telecom infrastructure, and overall security;
- c) **Personnel requirements** which are concerned with the technical competence of each TSTL staff member.
- d) **DUT Evaluation requirements** which are concerned with scheme related work
- e) **Operational requirements and obligations** which are concerned with day to day working of the TSTL

4.1.1 Conflict of interest requirements

4.1.1.1 The laboratory needs to be independent of its Parent company / Parent consortium members by incorporation. It shall, where applicable, deal with its parent/sister concerns at arms-length separation.

4.1.1.2 If the TSTL is controlled by a parent company, then the laboratory must demonstrate that there is sufficient separation of control and influence on the outcome of ITSAR evaluation activities. The laboratory shall demonstrate with objective evidences that:

- a) The parent company cannot exert undue influence on the outcome of the ITSAR evaluation activities
- b) Proprietary evaluation information cannot be inappropriately accessed by the parent company.

4.1.1.3 The laboratory must have procedures in place to ensure that management cannot exert undue influence on the outcome of ITSAR evaluation activities.

4.1.1.4 Under no circumstances, the same TSTL team or individual be involved in:

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 6 of 12

- a) both the development of the Telecom equipment and the conduct of its evaluation;
or
- b) provide consultancy advice to the client which would in any way compromise the independence of the evaluation.

4.1.1.5 TSTL staff may not engage in any evaluation activities on which they have previously acted as consultants, unless the TSTL can demonstrate that the independence of the evaluation will not be compromised. TSTL Staff cannot advise clients how to resolve problems, but they can comment on the adequacy of a proposed response or suggest possible options for consideration.

4.1.2 Facility Requirements

The following facility requirements are to be maintained by a TSTL:

- a) The laboratory must retain their evaluation and testing facilities permanently in India and have communication facilities like telephone (landline), Fax, e-mail ID, etc
- b) The laboratory must have sufficient office space and equipment space available. Also, space for at least one member of the Certification Body, for performing evaluation technical oversight, shall be made available, as and when required.
- c) The evaluation facility should be both physically and logically isolated from the rest of the organization with proper physical and logical security mechanism at the boundaries to ensure confidentiality of evaluation activities and their outcome.
- d) The laboratory must have or be able to provide sufficient IT infrastructure
- to support general documentation and for producing reports.
 - to protect documents from tampering
 - to maintain confidentiality of the reports
 - to access Internet (with adequate security measures)
 - to exchange evaluation objects and evaluation outcome securely with the client or validator/Certification body.
- e) The laboratory should have proper facility to protect the evaluation records and information used during the evaluation process.
- f) The laboratory must be equipped with necessary equipment, tools etc. relevant to the area of technology for which designation from DA is sought.

4.1.3 Personnel requirements

4.1.3.1 The TSTL shall have adequate staff with knowledge, experience and capable of performing ITSAR evaluations. The Laboratory shall also have personnel with industry recognised certifications in the area of IT/Telecom security testing.

4.1.3.2 Educational qualification for personnel performing Telecom security testing is given below for the purpose of reference:

Designation	Job Profile	Academic qualification	Experience in years
Test Engineer	Developing test design specifications, test cases, test suits etc.	B.Tech / B.E. in ECE/Computer science/ Telecommunications or MCA	min. 2 years;

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 7 of 12

Test Lead/ Test Manager	Developing Test Plan, Test Methods, review of test design specifications, test cases, test suits etc.	B.Tech / B.E. in ECE/Computer science/ Telecommunications; Industry recognised certifications in the area of IT/Telecom security testing is desirable	3 – 5 years
Technical Manager	Overall Responsibility of Technical operations	B.Tech / B.E. in ECE/Computer science/ Telecommunications; Industry recognised certifications in the area of IT/Telecom security testing is desirable	> 5 years
Quality Manager	Overall Responsibility of QMS activities of laboratory	B Tech, B E, MCA or equivalent	3 years

Note:

1.Laboratory shall have staff with appropriate qualification, certification, experience, etc. based on the Telecom equipment to be tested. In respect of core Telecom equipment testing, staff with adequate knowledge and experience in respective telecom technology shall be deployed.

2. In case the above functions are carried out by contract personnel,

a. The contract shall address:

- I. Responsibilities and authorities
- II. Confidentiality, integrity & indemnity requirements.

b. The laboratory is responsible for ensuring required qualification, experience, training, up gradation of the technology and domain related knowledge, etc.

4.1.3.3 **Authorised signatory:** The laboratory shall have minimum one authorised signatory who is responsible for:

- Authorisation for release of test reports
- Providing opinion and interpretations

The Authorized signatory shall have sufficient knowledge of :

- a. DoT Designation criteria
- b. ITSARs of Telecom equipment for the Designated scope
- c. Planning & designing of tests, analysis & reporting of test results
- d. standards or specifications, test methods and techniques
- e. the laboratory quality system;

Authorised signatory qualification and experience: Bachelor/Master degree in ECE/Computer science/Telecommunications Engineering, with minimum 10 years experience; Industry recognised certifications in the area of IT/Telecom security testing is desirable.

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 8 of 12

4.1.3.4 The laboratory shall have training procedure for staff covering:

- a. Laboratory Management System
- b. Evaluation specific domain/technology
- c. ITSAR requirements
- d. Operation of Test tools
- e. Operation of hardware and software at-site

Note: The laboratory shall inform the DA in writing if there is change in Authorised signatory as and when it occurs.

4.1.4 DUT Evaluation requirements

4.1.4.1 The laboratory must comply with requirements mentioned in “Procedure for Security Certification of Telecom Equipment – Doc.No. NCCS/SC/01 and the evaluation requirements as documented below:

- a) ComSeC Scheme Related Work: The TSTL must keep the Certification Body or its representative informed of all Test related work that is being performed.
- b) Registration for evaluation and Certification Services: The evaluation and certification process shall only be registered through the MTCTE process. In case the client contacts the TSTL in this regard, TSTL shall direct them to MTCTE portal.
- c) Evaluation Tasks: The TSTL must partition its work into discrete tasks. For the purposes of planning and reporting, a task corresponds to the work performed by a TSTL for the evaluation of a single Telecom equipment. A task must be uniquely identified throughout its life-time. The identification shall be such that the Telecom equipment and related items cannot be confused physically or when referenced in records or other documents.
- d) Supply of Documentation to the Certification Body: All documentation supplied by the TSTL to Certification Body must be in encrypted format through secure communication. In case the Certification Body has the facility to upload TSTL documentation on its portal, the same shall be followed by the TSTL as per the guidelines issued by the Certification Body.
- e) Appointment of Validator by Certification Body: The Certification Body may appoint a Validator as its representative for technical oversight of the evaluation process in the TSTL, if required. The TSTL shall provide access to Validator in its laboratory or other locations (when evaluation is done outside the laboratory) to allow him to observe and assess the evaluation being carried out by the laboratory.
- f) Task Initiation: The TSTL shall communicate to Certification Body or its representative when it is ready to perform an evaluation task.
- g) Task Confidentiality: Task information must be handled so that its confidentiality is maintained and the same is agreed upon through an agreement with the client. TSTL must ensure signing of confidentiality agreement with lab testing staff .
- h) Deliverables List: The TSTL must ensure that the client has contractually agreed to supply deliverables appropriate to the scope of evaluation.
- i) Evaluation Progress Reviews: Certification Body shall review directly or through its representative, all ongoing evaluation projects periodically.
- j) Task Records: For each task, the TSTL must ensure that a systematic record of all information is maintained in accordance with the TSTL’s Quality Manual.
- k) Observation Reports: TSTL must raise Observation Reports to draw attention of the client to deficiencies of the evaluation objects with respect to the requirements

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 9 of 12

of ITSAR and other problems, as and when they are discovered, during an evaluation and communicate the same to the client securely.

- l) Evaluation Work Sheets: TSTL shall document the evaluation results in the form of work sheets addressing the results of evaluation in respect of ITSAR. The same shall be presented for validation by Certification Body, if required.
- m) Evaluation Report: The TSTL must produce a final Evaluation Report and supply a copy to Certification Body. The TSTL must report the work performed and the detailed results in the Evaluation Report, giving sufficient justifications for verdicts and conclusions.
- n) Test records: TSTL must ensure that scripts for penetration tests and additional implementation tests are recorded in sufficient detail to allow repeatability and reproducibility. When a tool is used to assess one or more test items this must be recorded in sufficient detail to allow repeatability or reproducibility.
- o) Closure: When the TSTL has completed the evaluation work and the Certification Report has been agreed and issued, the TSTL can close down the project. In the closure process, TSTL shall archive or dispose of all material supplied for the evaluation as decided in initial meeting with the client. Adequate records shall be retained by the TSTL to ensure the reproducibility and repeatability of the task.

4.1.4.2 Security evaluations may be conducted at the developer site (if located in India), the laboratory or another location (in India) that is mutually agreed to by the TSTL, the developer, and Certification Body, in exceptional circumstances. When evaluation activities are conducted outside the laboratory, the laboratory shall have additional procedures to ensure the integrity of all tests and recorded results. These procedures shall also ensure that the same requirements that apply to the laboratory and its facility are maintained at the non-laboratory site.

4.1.4.3 Laboratory shall not further subcontract the evaluation activity including testing in part or full to any other agency for which lab is designated.

4.1.5 Operational requirements and obligations

4.1.5.1 The TSTL shall implement a clear procedure for resolving client complaints and disputes. Upon the Certification Body's written request, the TSTL shall make available to the Certification Body details of the nature of any complaints made against it and, where applicable, the resolution thereof. The TSTL shall take such corrective action as the Certification Body may require in respect of or as a result of any complaint.

4.1.5.2 The TSTL shall comply with all applicable laws and obtain and maintain all licenses, consents, permits, approvals, waivers and authorizations necessary for the evaluation activities and the performance of its obligations.

4.1.5.3 The TSTL shall ensure that all information it provides about itself or its services and fees are true, accurate and complete and promptly provide updates to such information as and when necessary.

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 10 of 12

4.2 Evaluation activities of TSTL

4.2.1 Scope

4.2.1.1 The evaluation activities of TSTL shall include performing specific tests to verify whether the particular Telecom equipment meets all the security requirements as specified in the ITSAR of that particular Telecom equipment.

4.2.2 Areas of Security Testing

4.2.2.1 The areas of security testing shall broadly include (wherever applicable) but not limited to the following:

- a) Access and authorization
- b) Authentication attribute Management
- c) Software security
- d) Source code review
- e) Secure execution environment
- f) Security audit (audit trail generation and secure storage, etc)
- g) Data protection (implementation of cryptographic services)
- h) Secure network services
- i) Attack prevention mechanisms
- j) Vulnerability testing requirements
- k) Operation system security
- l) Web server security
- m) Telecom equipment specific requirements

4.2.2.2 The latest version of applicable ITSAR(s) for Telecom equipment may be referred to for the areas of security testing applicable for that Telecom equipment.

4.2.3 Test methodologies and validation

4.2.3.1 The laboratory shall take into consideration, wherever available, international standards referred to in ITSAR and/or evaluation guidance issued against ITSAR in respect of security requirements and formulate test procedures for conducting security evaluations. The laboratory shall, in general, be able to formulate test procedures based on the security requirements specified in ITSAR.

4.2.3.2 Techniques to be used for evaluation of security features of the Telecom equipment shall include, but not limited to, the following:

- a) Analysis of report on tests carried out by Vendor/OEM against ITSAR
- b) Analysis of Telecom equipment documentation provided by Vendor/OEM that are essential for performing testing as per ITSAR
- c) Testing of Telecom equipment to verify that it meets ITSAR requirements

4.2.3.3 The testing approach to be followed by TSTL should clearly address the following:

- a) Complete coverage of all the ITSAR requirements that the Telecom equipment is expected to comply with
- b) Test plans for every ITSAR, equipment and resources to be used, pre-processing and post- processing necessary for the test, etc.
- c) Detailed test procedure

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 11 of 12

- d) Alternative Test approach, if any, with the approval of Certification Body
- e) Expected result
- f) Actual result

4.2.4 Proficiency Testing

4.2.4.1 Proficiency Testing will form part of the designation process wherein the TSTL shall demonstrate its competence in performing testing ITSAR requirements to the DA. The proficiency test consists of the laboratory conducting an evaluation in accordance with ITSAR requirements for the applicable scope for which designation is sought. Successful completion of the evaluation is a requirement for initial designation as well as continuing designation.

Document	Designation Requirements for Telecom Security Testing Laboratories				
Doc No.	Issue No	Issue Date	Revision No	Revision Date	Page no.
NCCS/SLR/03	1.0				Page 12 of 12