11-1/2020-TTSC
Ministry of Communications
Department of Telecommunications
(Security Assurance Wing)

Room No 724, Sanchar Bhawan
Dated 04.04.2024 at New Delhi

Office Memorandum

Subject: Clarifications emerged after the meeting held under the Chairmanship of Member(S) on 04.03.2024 to discuss the issues raised by Industry and OEMs regarding COMSEC scheme.

A meeting was held under the Chairmanship of Member(S) on 04.03.2024 regarding the subject matter. In this regard, clarifications against each issue are enclosed herewith for ready reference.

2. This is for kind information and necessary action.

Encl: as above

Digitally signed by NISHANT CHAUDHARY
Date: 2024.04.04 10:59:30 +05'30'

(Nishant Chaudhary)
ADG (TTSC)
Email: adg.ttsc-dot@gov.in
Tele: 2332-9236
2303-6410

To,
All participants (thru email)

Annexure-I

List of Participants:

Sl. No.	Name	Designation	Organization
1.	S. N. Rama Gopal	Sr. DDG NCCS	NCCS
2.	P. K. Singh	DDG (SA)	DoT HQ
3.	K. Srikrishna	DDG (SAS)	NCCS
4.	R. Bala Srinivasa Kumar	DDG (SAD & HQ)	NCCS
5.	Khushboo Sharma	Director (UDS)	DoT HQ
6.	Nishant Chaudhary	ADG (TTSC)	DoT HQ
7.	Vikram Tiwathia	DG	COAI
8.	Priya	Dy. Manager	COAI
9.	Jyoti Chawla		Nokia
10.	Amit Anand		Nokia
11.	Vibha Mehra		Nokia
12.	Anita Kumar		CISCO
13.	Sandeep Goel		CIENA
14.	Amol Madan		Ericsson
15.	Jagdeep Walia		Ericsson

Annexure-I

Clarifications against issues raised by Industry and OEMs regarding COMSEC scheme:

**Test reports from ILAC/third party labs wherever applicable under this document are acceptable barring reports of test labs from land bordering countries.*

Sl. No.	Issue	OEM/ COAI recommendations	Clarifications by DoT
1.	**Source Codes: Submission for testing**	For OEMs to obtain source code for review with a designated TSTL (Telecom Security Testing Lab, a DoT accredited third party lab) as mentioned in all ITSARs has been strongly opposed during various industry deliberations. Source code is proprietary by respective vendors and related to their IPR, it is not possible to share the same. As an industry-best practice, it is not recommended to possess or have any access to source code, as it could lead to security breaches. Furthermore, even the internal Test Report related to Source Codes cannot be shared with any third party as per the industry standards. **Recommendation: it is necessary to permit the industry to submit the undertaking or self-declaration on authentication of the Source Codes instead of obtaining the Source Codes or any internal Test Reports.**	(a) Industry submitted that neither source code nor internal test Report of the source code can be submitted, not even under NDA (b) NCCS informed that for EAL-4 and above security certification testing of source code is mandatory. Reference of EU and Netherlands document was cited by NCCS. (c) It was decided that after the launch of mandatory certification, DoT will accept internal test report/Software Test Document in this matter up to first 6 months after that source code submission shall be mandatory for testing and certification (d) Source code submission for testing of IP Router, Wi-Fi CPE is not envisaged in ITSAR at present. The same shall be incorporated after the modification of ITSAR's or one year whichever is earlier. Till such time the OEMs may submit internal software test reports/third party software test

			reports/ILAC Test reports to NCCS/recognized test lab under an NDA **barring labs from land bordering countries** (e) Test report submitted for a product should pertain to the software release (X.Y) which has been applied for testing & certification. In case, during the course of testing, there is a change in software release (X+1.Y or X.Y+1 or X+1.Y+1, the increment in major.minor (X.Y) release may be any amount of change, need not necessarily be limited to 1 only), it is assumed that no software test report exists for the new software release, hence the applicant/OEM has the option of submitting the new release **for further testing** with an undertaking that no vulnerability exist in the new source code/Software release.
2.	**Evolving Lab Infrastructure**	Over the last few years, the lab infrastructure under MTCTE has evolved gradually. For security testing, there are only three accredited labs. There are more in the pipeline, but you will acknowledge that OEMs will hesitate to enter commercial engagements with labs till they are completely audited and accredited for all testing requirements. Considering limited labs, testing costs are very high	(a) It is expected that the market will self-regulate the test fees when number of labs increases further. (b) Industry highlighted that despite the increase in number of labs, Cost of testing has not been reduced by the labs.

		and significant delays can be expected (range of INR 40-60 lakh per model). **Recommendation: The industry requests that these costs and timelines are considered before mandating the scheme. The labs must also reconsider the costs, considering a lot of products will be notified in the future.**	(c) Industry requested for market monitoring of labs by DoT w.r.t cost effectiveness. (d) NCCS will not charge any fee (administrative & assessment/evaluation) for the extended period of voluntary testing till 31st March 2024 or till such further period as notified for voluntary Security testing and certification. (e) Industry to bring more product for testing
3.	**Lack of testing ecosystem in India**	It is significant move that NCCS has recently setup 2 more labs in addition to the existing lab with suitable capacity and also allowed voluntary testing till 31st December 2023, to cater the behemoth requirement of testing and certifying of numerous telecom network equipment under ComSec scheme. However, due to unavailability of sufficient number of labs with required capacity and capabilities may lead to sever bottleneck which will impact the ongoing deployments of network elements in Telecom Network deterring the coverage and quality to the end users. **Recommendation**: **It is requested to keep the ComSec testing and certification on voluntary basis instead of mandating the same until the necessary testing labs and ecosystems are established in India.**	(a) 4 Labs have already been designated. (b) DoT HQ and NCCS are proactively striving for designating more labs for this purpose.

4.	**Known Malware checks**	OEM are required to submit an undertaking stating that product is free from all known malware and backdoors as on the date of offer of product to designated TSTL for testing and also submit their internal Malware Test Document (MTD) of the product to the designated TSTL. Since there will be lag between the time the product is released by OEM and the actual time it is offered for testing, hence we request to change the requirement to "at time of product release" rather than “from date of offer of product to TSTL for testing”. **Recommendation: It is requested that the industry submit the undertaking instead of obtaining the necessary internal test reports.**	(a) Till the availability of test tools with TSTL, the reports from ILAC test labs/internal test lab/third party lab (barring labs from land bordering countries) may be shared under NDA which the TSTL/NCCS shall examine and process for certification, after ascertaining the completeness/correctness. In case of non-submission of security test reports/Malware Test Document as above, the TSTL/NCCS shall perform malware checks and provide reports. (b) In case the software release is not more than three months old from the date of submission, the applicant/OEMs may submit an undertaking that the software release is free from known **Malware** as on the date of software/product release **or submit the** test reports from ILAC test labs/internal test lab/third party lab (barring labs from land bordering countries) **before issue of certificate.**
5.	**Vulnerability Scanning**	We would like to mention that producing software that is free of all known vulnerabilities is near impossible feature. The current best practice in the industry is to conduct comprehensive risk assessments based on the categorization of the severity of potential security vulnerabilities. The industry request that the treatment of known vulnerability closure should be based on the classification. The industry is addressing all	(a) It was agreed that before final certification, telecom equipment shall be free from known critical and High vulnerabilities. There would be a road map provided to address the detected known medium and low vulnerabilities. (b) In case, there is a need to submit a new release as defined in para 1 above and/or , Build/bug fix update/upgrade

		the known critical vulnerabilities before releasing any new commercial software. Expectation to fix all vulnerabilities will consume considerable efforts / time and also run the risk of losing attention of the critical vulnerabilities. **Recommendation: It is requested that a remediation plan for addressing high and medium-known vulnerabilities should be provided by industry.**	to take care of detected critical/high vulnerability during the course of testing, the same may be submitted along with an undertaking as in para 4 which will be tested and certified in lieu of the old release.
6.	**Software Upgrades/Patches/Bugs/Fixes**	Repetitive testing of every software patch or update /upgrade on regular intervals should be exempted from the certification process under the integrated regime of MTCTE. Since it is understood that the cycle of testing & certification goes from 6 months to 1 year, and the frequency of updates can be between 2 weeks to 3 months depending on the requirement of network. Therefore, every Software upgrade/updates cannot be certified. Sometimes, in the event of emergency, a fix is required to be applied in the network and it cannot wait for the complete cycle of ITSAR testing or certification. **Recommendation: It is requested to permit the industry to submit the undertaking on subsequent Software Upgrades/Patches/Bugs/Fixes once the Software has been certified by NCCS for 10 years.**	a) **After a product has been certified for first time, release of new updates/patches/bugfixes/upgrades/ new builds etc. will be allowed to be deployed for a period of upto two years (from the date of initial certification) without further testing based on the declaration by the OEM that such releases does not impact the security posture of the product, and submission of internal test report/Impact Assessment Document for the relevant main models** (b) NCCS to explore whether for the next release common parameters testing for which testing was done for the older release can be avoided and limited testing of specific new added features (new versions) can be done to save time and resources. The same can be ascertained through OEM documents on release/bugfix details.

			(c) The process may be reviewed depending upon the product and learnings from the test.
7.	**Different hardware models using the same software**	A particular Software that is used across multiple or different Hardware's should go for an integrated MTCTE certification only, which is valid for 10 years from the issuance date of certificate. Since ITSAR is entirely about tests on Software and rarely on hardware, hence testing of any single member of family should suffice, for a complete family's certification. **Recommendation: In order to avoid the repetitive testing of same Software used across different Hardware's, it is requested to test them only once and certify all the related Hardware utilizing the same Software. Also, installed base (old model) in the network which still has book value of 7-8 year but is not part of the new supply, should be exempted from the need for ITSAR certification.**	**(a) Security testing done for a software release (X.Y) in the highest physical configuration of a product will be applicable for sub-products having lower physical configuration & the same software release in the main/associated models of product also. Release of new updates/patches/bug fixes/upgrades/new builds etc. will be allowed to be deployed for a period of upto two years (from the date of initial certification) without further testing based on the declaration obtained from OEM submitted by the OEM/applicant that such releases does not impact the security posture of the product, and submission of internal test report/Impact Assessment Document for the relevant main models** (b) **For the products having same software release and pertaining to different main/associated models, NCCS may re-examine testing of only those parameters, which are different, if applicant/OEM is able to demonstrate common set of ITSAR**

			requirements in both the main/associated models. This kind of mapping will only be done after written submission from the OEMs. (c) **CIENA** intimated that they have been using single software across different families of products, CIENA was requested to submit Application for two different families of products having similar Software to NCCS for study and finalising testing requirements
8.	**Unnecessary Services Removal/ Unused Functions/ Unsupported Components or Software's**	There are instances where the platforms provide different software/services in the node. These functionalities in the nodes are enabled during commissioning of the node as per Customer requirement. In such cases, unused software/services will remain in the system, but will not be used until the activation is complete. As the Software for a particular product is always tested from all aspects, including security, it is not feasible to set up and obtain it tested for each version. Furthermore, there are a few features/functionalities that may or may not be required by one Customer, but may be required by another, thus it is necessary to remain in the system. **Recommendations: It is recommended that any change or modification must be authorized by the highest-level designated authority in order to implement the desired features/functions.**	(a) The unused software services/components/interface etc. are to be disabled/deactivated at the time of product submission for testing. This is feasible without leading to a change in the original release already tested or submitted. It is a situation similar to lower configuration of product in a family which has already been covered in para 5-7. (b) It was suggested that certificate issued by NCCS may contain following clause: - *' XYZ features/components were disabled during the testing, enabling of which may result in a vulnerability. Responsibility of breach due to enabling of this particular feature/component shall lie with the entity which have enabled this feature/ component.*

			(c) Further, the list of features which are disabled shall be attached with the final certificate
9.	**FIPS Compliance**	ITSAR mandate for Cryptographic algorithms and modules to be compliant with FIPS 140.x. Most of the Crytpo algorithms and modules implemented in product are sourced from open source. FIPS-140 certification/compliance is needed for Defence/military deployment and not a typical requirement for telecom equipment. It will require a considerable amount of effort, and cause delay to implement FIPS compliant crypto engines. **Recommendations: It is recommended that this compliance is not required to be provided for the Licensed Telecom Services in the country.**	(a) Submission of an undertaking from the OEM that "the crypto module implemented is in compliance with FIPS 140-2 standards" is required along with application was agreed to. In absence of such undertaking the crypto/third party modules can be got tested by OEM to ensure compliance in line with FIPS 140-2 standards. Such test reports from ILAC test lab/internal test report/third party(barring labs from land bordering countries) /CDAC, Bangalore may be agreed to by NCCS till adequate capabilities get developed in the country." (b) Submission of undertaking by OEMs for a new release during three months prior to application can be done **before issue of certificate** (c) NCCS to examine the cost and time of FIPS testing.
10.	**Test parameters**	Presently, ComSec requires compulsory clearance of all security test parameters for certification. To provide context, Wi-fi CPE has 77 test parameters and IP Routers have 82 test parameters under their respective ITSARs. Considering the dynamic nature of software, it becomes challenging for OEMs to conform to each test parameter in its entirety.	(a) "ITSARs *contain common requirements and specific requirements for a product. NCCS may consider launch of security testing of all 5G NE with common security requirements till testing capabilities pertaining to specific requirements get developed in the country."*

		Industry requests DOT/NCCS to consider this challenge and have levels of clearance – 'good to clear' or 'must clear' – to reduce compliance burden and ensure certification.	(b) The process may be reviewed after one year from date of implementation of mandatory testing
11.	**Aggressive Timelines**	NCCS has announced January 1, 2024, as the start date for acceptance of application for IP Routers and Wifi CPE. However, there are only 3 labs accredited by NCCS to perform the Security testing. Further there are still many ambiguities in the ITSAR and the **test procedures have not been defined by NCCS** for the labs. Industry can comply with the security testing and certification requirements only after NCCS accredits sufficient labs, removes all the ambiguities in the ITSAR and clearly defines the test procedures. **Recommendation: we request DoT to not mandate the security requirement testing and certification until these issues are resolved. Further, learning from the experience of MTCTE, industry strongly urges DoT to provide a minimum of 2 years to comply with the security testing requirements.**	(a) Timelines have been already extended by 3 months i.e 31st March, 2024 (b) NCCS to examine and record time taken in each test out of 82 parameters and push labs to reduce time of testing (c) Industry to offer more product for testing.
12.	**Timelines for Testing Cycles**	As per NCCS SOP, it is mentioned that the time required for Security testing/certification is likely to be at least 6-7 months. This does not include activities such as the Lab engagement/ contractual agreement time, Time slot availability,	Timelines have been extended by 3 months.

		Logistics for equipment & competent resource availability, etc. **Recommendation:** i Firstly, all the activities put together shall at least require a minimum of 1 year from the date of mandatory notification to the final certification. ii Secondly, the Voluntary certificate program should be extended for one year.	
13.	**HSE Exemption**	TEC, on 18th April, 2023 issued an exemption for equipment having specialized test requirement under MTCTE (AC current requirement >32A or DC current requirement >100A). **Please confirm that the exemption contained in this notification No. 6-6/2021-TC/TEC (Pt II) is applicable for ITSAR testing as well.**	HSE exemption matter shall be handled by Sr. DDG (NCCS) on case by case basis. The tests, which require product as DUT, shall be governed by HSE exemption. However, tests of software/release/source code etc. does not require the HSE exemption and may be done as per normal test procedure as applicable.