PHD House, 4th Floor, Ramakrishna Dalmia Wing
4/2, Siri Institutional Area, August Kranti Marg, New Delhi – 110016,
Tel# 9355144223 E-mail: dg@mait.com □ Website: http://www.mait.com

Ref.No.MAIT/PY/2327 November 07, 2023

Dr Neeraj Mittal, IAS
Chairman DCC & Secretary (T)
Department of Telecommunications

Subject: Seeking support on ComSec implementation

Respected Sir,

Greetings from MAIT, India's apex body empowering IT, Telecom & Electronics Hardware Sectors!

At the outset, MAIT and its members would like to thank the Department of Telecom for the continued support in MTCTE regime. On similar lines, we would like to draw your kind attention to **Communication Security Certification Scheme (ComSec),** a part of the MTCTE scheme which mandates any telecom product sold or imported in India needs to be tested and certified for security requirements.[1] The nodal agency for implementation of the scheme is National Centre for Communication Security (NCCS).

The testing requirements are defined under the Indian Telecom Security Assurance Requirements (ITSARs). **Products in ComSec Phase-1 are as below:**

1. IP Routers
2. Wi-Fi Customer Premise Equipment (CPE)

Timelines for ComSec Phase-1 (as on date):

1. Mandatory application date on the portal is January 1, 2024.
2. Voluntary applications accepted from September 1, 2023. The application form and submissions to be made in hard copies.

Industry Key issues:

1. **Strict Timelines:** NCCS has announced January 1, 2024, as the start date for acceptance of application for IP Routers and Wi-Fi CPE. However, there are only 2 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. Therefore, **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 requests DoT to provide a minimum of 2 years to comply with the security testing requirements.**

2. **Product Grouping:** As per the MTCTE procedure, the family grouping is done as per hardware similarity. However, ComSeC is a software security testing certification. Therefore, the MTCTE grouping is not ideal for software security testing. You will agree that several similar networking products are deployed with the same software. Therefore, testing based on MTCTE grouping is challenging for security testing. According to current NCCS procedures (based on MTCTE), OEMs are mandated to repeat testing of the same software across similar hardware. There is no separate grouping recommended under ComSec scheme. Repeat testing would have a

[1] https://117.196.240.24/nccs/

significant cost implication on the industry. ***The industry requests DoT and NCCS to review this requirement and allow certification of all hardware models running the same software, basis test report of the software on any one of the hardware models.***

3. **Repeat testing for every SW patch/upgrade/update:** You would appreciate that software of any product undergoes periodic updates, upgrades sometimes within a span of a few weeks to months. However, repeat security testing and certification for each upgrade/update is not feasible. Further, every test and certification cycle can go from 6 months to a year, which is impossible to achieve for each update, upgrade. ***It is requested that this requirement should be exempted and the certification should remain valid for 10 years without testing requirement in between. Alternatively, the OEM can also submit an undertaking on subsequent Software Upgrades/Patches/Bugs/Fixes once the Software has been certified by NCCS for 10 years.***

4. **Vulnerability Scanning:** You would acknowledge that developing software that is free of all known vulnerabilities is a 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 requests that the treatment of known vulnerability closure should be based on the classification. The industry can only fix all the known critical vulnerabilities before releasing any new customer software. ***The industry requests that if industry can provide a remediation plan for addressing high and medium known vulnerabilities. The expectation to fix all vulnerabilities will consume considerable effort / time and run the risk of losing attention of the critical vulnerabilities.***

5. **Source code submission** – As the ComSec security scheme requires the source code to be made available in the notified labs for the testing purposes, industry shared the reservations on the same due to security concerns. As per the best practices across the globe, it was suggested to have "Scheme based on GSMA NESAS where 3*rd* party auditors assess whether vendors have processes in place around secure code development, source code review and testing within the vendor R&D teams". ***Industry requests the above suggestion to be followed in the country also.***

6. **Evolving Lab Infrastructure:** Over the last few years, the lab infrastructure under MTCTE has evolved gradually. For security testing, there are only two 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 (range of INR 40-60 lakh per model) and significant delays can be expected. ***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.***

7. ***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. ***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.***

We are sanguine that our request will merit your positive consideration.

Warm regards,

Col Suhail Zaidi (Retd)
Director General

CC: Shri R R Mittar, Advisor & Head, TEC
CC: Shri S N Rama Gopal, Sr. DDG, NCCS
CC: Shri Anand Katoch, DDG (TC), TEC