MAIT

PHD House, 4th Floor, Ramakrishna Dalmia Wing
4/2, Siri Institutional Area, August Kranti Marg, New Delhi – 110016,
Tel# 9599665859 E-mail: ajafari@mait.com □ Website: http://www.mait.com

Ref.No.MAIT/PY/2680 April 06, 2023

Shri K Rajaraman, IAS
Chairman-DCC & Secretary
Department of Telecommunications

Subject: MAIT Representation on Security Testing of Wi-Fi CPE and IP Routers under Notification No.1-6/2022-TC/TEC

Respected Sir,

Greetings from MAIT!

MAIT would like to thank DoT for patiently hearing the pain points of the industry in the past and giving the much-needed relaxations by first scrapping the regulatory overlaps that existed between CRO and MTCTE, then by extending the timelines of the Phase 3 & 4.

We write this representation to bring to your kind attention our members' latest concerns with the TEC Notification No.1-6/2022-TC/TEC issued on February 27, 2023, with the subject line "*Notification of Wi-Fi Customer Premise Equipment (CPE) and IP Router including security testing under MTCTE-regd.*" We are optimistic that, like in the past, your good offices would act immediately and take necessary actions on industry recommendations.

We would like to reiterate that MAIT and its members stand totally united with the Department of Telecommunications' vision and objectives laid down under the MTCTE regulations and have been extending full cooperation since the inception in building and achieving a robust regulatory governance system. However, our members have noted several challenges in the Communication Security Certification (ComSeC) Scheme of National Centre for Communication Security (NCCS), which if not evaluated, can bring severe implications on the industry.

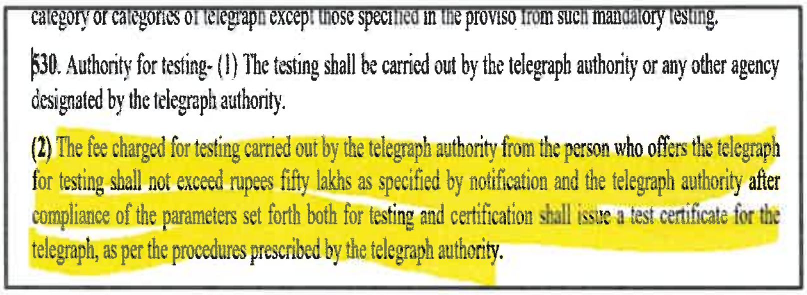
From our perspective, the TEC's notification of Feb 2023 would have serious repercussions on the way the industry can do business in India and can deter our country's economic growth. We have emphasized underneath some of the key concerns that we foresee and have recommended some suggestions for your kind consideration and immediate action:

Industry's Concern	Recommendation:
1. Industry's Concern: Short Deadlines with Lack of testing infrastructure and Accredited Labs • TEC on 27th Feb 2023 has announced the start date of security testing and certification for Wi-Fi CPE and IP routers as July 1, 2023, giving the industry merely 3 months to comply. • As of March 20, 2023, there is **only one lab** accredited by NCCS to do the security testing. • NCCS has still not finalised the test procedures and the test report format which are essential for the labs to initiate the testing. Without these the labs are non-committal on the testing timelines and have denied quoting the testing costs. Our members have been informed that the lab has requested NCCS to finalize the approach on ITSAR testing and the lab expects to have clarity only by end of March 2023. Until then the lab is not even able to give the cost	• MAIT believes it is practically not possible to meet the security testing and certification requirements starting July 1, 2023. We fear the businesses will come to a grinding halt if the effective dates are not extended. It is important that we learn from the experiences of the MTCTE and do not repeat the same mistake that we did while launch of the MTCTE Phase 3 and Phase 4 of giving inadequate implementation time to the industry to comply with. **We recommend DoT to give sufficient time to the industry to comply with such a complex testing regulation. DoT must ensure all the required infrastructure are in place**

quote / commit testing timelines. Please find attached an email communication received from the only lab accredited to do security testing as **Annexure-A**. • As per another lab (which is not yet accredited), the time required for testing per model is approx. 14 weeks (3.5 months). Pls find attached the email communication from the lab on the testing timelines and costings as **Annexure-B**. Once the product is tested, we assume NCCS would need at least 4 to 8 weeks to review the test reports and issue the certificate. . Which means once the NCCS finalises the ITSAR testing procedure, the lab and NCCS alone would need minimum 5.5. to 6 months to perform testing and certification. This does not include the sample arrangement time or the pre-testing wait time at the labs.	**before enforcing any regulation. We request DoT to extend the timelines for Security in-country testing and certification by at least 2 years i.e. until July 1, 2025 for the notified product categories.** • We further hold the view that industry can comply with the security testing and certification requirements even by July 2025 only after NCCS accredits sufficient labs, remove all the ambiguities in the ITSAR and clearly defines the test procedures. We request DoT to not mandate the security requirement testing and certification until the testing ecosystem with sufficient labs are established in India. • In addition to this, we would like to request DoT and NCCS to ensure that any edits in the ITSARs do not lead to expansion of the product categories to include multiple other technologies within the same ITSAR. This will severely disrupt the current testing cycles and would cause delays. • We further believe that any new product/phase of products must be mandated only after the capacities – ITSARs and labs – are duly evaluated and sufficient numbers of labs are ready, as it may disrupt the current testing timelines of the first phase products.
2. **Industry concern: Ambiguous standards** • Concern #1: While ITSARs mandate the requirements for testing, they are still unclear about the methodologies/approach/procedure to be adopted by TSTLs to conduct testing. In such a scenario, TSTLs are dependent on NCCS to provide them case by case/ITSAR by ITSAR approvals for methodologies, which are time consuming. All ITSARs must be entirely clear in terms of both testing requirements and methodologies before the commencement of tests. • Concern #2: Though NCCS has stayed engaged with industry on updation of ITSARs, there are still many concerns that exists across the ITSARs which are challenging for the industry to comply with. For example, in the IP Router ITSAR, there are three concerns: • Clause no: 3.3 Source code security assurance • Clause no 3.4 Known Malware Check • Clause 9.1: Fuzzing – Network and Application Level It must be acknowledged that producing software that is free of all known vulnerabilities is near impossible feat. The current best practice in the industry is to conduct comprehensive risk assessments based on the	**Recommendations:** • Recommendation #1: NCCS must publish test case description and standardised procedure/methodology for testing for each ITSAR requirement or as Implication Notes to ensure there is clarity among all TSTLs. • Recommendation #2: Industry believes that NCCS must reconsider these requirements and accept OEMs' declaration on the aforementioned clauses

	categorization of the severity of potential security vulnerabilities.	
3.	**Industry's Concern: Product/Family groupings** • In the MTCTE procedures, TEC has given guidance on the associated models and family grouping which helps the OEM on clubbing a series of models in one family, basis the hardware design/configurations. • However, the NCCS has defined the product grouping as below (Clause 4.3 of the certification guidelines) *The model with full configuration of hardware, interfaces and software is called the Main model. Associated models for the purpose of Security certification are those models which have identical software but having hardware which is a subset of the main model. Associated models of the telecom equipment shall be certified without testing.* The challenge of the industry is that for two or more main models, the software could be same. Under the current NCCS procedures, such products may not / could not be grouped in one family, which would lead to repeated testing of the same software (which defines the security of the product). The repeated testing would have a huge cost implication on the industry.	• We request NCCS to develop associated model/family grouping guidelines on basis of the products' major software versions. Change in the hardware/cryptographic chip should not call for retesting/recertification. OEMs should be given the flexibility to decide the minimal set of products to be tested and certified, with an undertaking / Declaration of Conformance (DoC) for rest of their models in the family as compliant. • Provision of software updates and bug fixes/patches is a continuous process, and the product cannot be expected for renewal/ recertification within these cycles of software updates and bug fixes/patches. Once tested and certified, no further renewals or recertifications need be done except for major software releases. Perhaps the authorities can have confidence that the OEM would keep a record of the software updates.
4.	**Industry Concern: Very broad product scope:** • The ComSeC Scheme mentions that it is applicable on all telecommunication equipment for which MTCTE applies. While we understand the importance of safeguarding the security of India's public network, it is equally important to create policies that endorse, rather than hinder, ICT trade and promote ease of doing business. • Mandating the Security Testing and certification on all MTCTE products will not add any value to India's public telecom network, rather it will further increase compliance burden on the already over-regulated ICT and telecom sector. • A lot of products intended to be covered under the mandatory Security Testing and Certification do not have the capability to connect to the public network directly, example Access Point. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. Access Points support the connection of multiple wireless devices through their one wired connection. An Access Point serves as the interconnection point between the WLAN and a fixed wire network. Access Points do not connect to any telecom network directly. Further, products that Access Points connect to - like Switches or Routers, are anyway regulated under the security testing, we believe Access Points should not be mandated for security testing.	• We request DoT to limit the scope of the Security Testing to products that can be directly connected to the Indian telecom network or licensed operator's network or service provider's network and have potential security risk. • Ensure Consistency with Globally Aligned Definitions. The definition for Wi-Fi Customer Premise Equipment (CPE) in the security assurance standards (SAS) is unclear and should be aligned further with common definitions, such as 3GPP and European Telecom Standards Institute (ETSI) standards[1]. We recommend that DoT/NCCS narrowly define "Wifi customer premise equipment (CPE)" to equipment at the end user's premises primarily on routers and gateway devices which connect directly to the network. **Devices such as access points or client devices/IoT devices should be out of scope.**
5.	**Industry Concern: Exorbitantly high testing costs**	• Majority of the products must be tested immediately and if the testing costs are

[1] Access, Terminals, Transmission and Multiplexing; Third Generation Transmission Systems for Interactive Cable Television Services – IP Cable Modems: DOCSIS3.0 EN 302 878-3 V1. 2011.

• As per our understanding, the cost for security testing of a Wi-Fi CPE is **₹51 Lakh** + 18% GST and that of an IP Router is **₹55 Lakh** + 18% GST**,** which totals up to **₹60 Lakh to ₹66 Lakh.** Please find attached a quote from one of the labs. In addition to the above, the OEMs currently pay approx. (₹17 Lakh to ₹21 Lakh for testing other parameters of the MTCTE ER (i.e., safety, EMI/EMC, and technical parameters). With the security testing getting mandated, going forward the OEM would have to pay approx. **~₹76 Lakh to obtain a MTCTE certificate.** • As per the Indian Telegraph Amendment Rules 2017, *"the fee charged for testing carried out by the telegraph authority from the person who offers the telegraph for testing shall not exceed INR 50 Lakhs as specified by notification…"*  category or categories of telegraph except those specified in the proviso from such mandatory testing. 530. Authority for testing- (1) The testing shall be carried out by the telegraph authority or any other agency designated by the telegraph authority. (2) The fee charged for testing carried out by the telegraph authority from the person who offers the telegraph for testing shall not exceed rupees fifty lakhs as specified by notification and the telegraph authority after compliance of the parameters set forth both for testing and certification shall issue a test certificate for the telegraph, as per the procedures prescribed by the telegraph authority. • We understand that the maximum testing cost defined in the Telegraph Rule is for the complete MTCTE testing, which includes Safety, EMI/EMC, Radio, Technical Parameters + SECURITY parameters. However, currently the testing costs charged by the labs outstrips this maximum capping. There is no standard price defined or regulated by the department which gives a leeway to the labs to charge arbitrary testing prices. Further, because there are very few labs available for testing, a monopolistic market is being created. OEMs have no choice but to agree to arbitrarily high testing costs quotes by these labs. • We fear the high testing costs would act as a barrier to trade and would lead to creation of monopoly.	not brought down, it will only aggravate the problems of the industry which is going through a rough patch due to the declining revenues, mounting debt, hyper-competitive marketplace. • MAIT, therefore, respectfully requests **DoT to regulate the testing cost immediately and not wait for the market forces to drive the prices.** • Further DoT should also ensure there are sufficient labs accredited to avoid monopoly in the market.

We look forward to your positive consideration of our recommendations.

Warm regards,

Col. AA Jafri, Retd
Director General

CC: Shri S K Jain, Member-Services, DoT
CC: Shri Ritu Ranjan Mittar, Sr. DDG, TEC
CC: Shri S N Rama Gopal, Sr. DDG, NCCS