PHD House, 4th Floor, Ramakrishna Dalmia Wing
4/2, Siri Institutional Area, August Kranti Marg, New Delhi – 110016, India
Tel#: (+91-11) 2685 5487 • Fax#: (+91-11) 2685 1321
E-mail: ceo@mait.com • Website: http://www.mait.com

Ref.No.MAIT/PY/2238 November 19, 2020

Shri Anshu Prakash
Secretary
Department of Telecommunications

Subject : Industry inputs on the concerns related to NCCS - ComSeC Scheme.

Respected Sir,

Greetings from MAIT, the apex body of the Electronic Hardware Manufacturing Sector in India!

The ICT Industry stand aligned with the Department of Telecom's regulatory goals under the MTCTE procedures and have been extending our full cooperation since the genesis, in developing and implementing a regulatory governance system. We are committed to work with DoT and believe our recommendations will contribute in safeguarding the safety, security and performance of the public telecom network.

As you would be aware, when the MTCTE procedures were published in October 2018 it mandated testing and certification of telecom equipment as per the essential requirements. The essential requirement developed by TEC covered (a) EMI/EMC (b) Safety (c) Technical requirements (d) other requirements and **(e) Security requirements.** The telecom equipment is required to be tested against these requirements and get an MTCTE certificate from TEC. However, DoT has implemented the mandatory testing and certification in respect of Security Requirements through a new scheme titled *'Communication Security Certification (ComSeC) Scheme'* and National Centre for Communication Security (NCCS) shall be responsible for implementation of this scheme. We are deeply concerned with this parallel certification scheme being rolled out by NCCS/TEC/DoT.

Industry's main challenges and concerns with respect to *ComSeC Scheme* are as below:

1. **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 *ComSeC Scheme* 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 industry. A lot of products intended to be covered under the *ComSeC Scheme* do not have the capability to connect to the public network *directly*. Such equipment are low in security risks.

   Industry Request: We request DoT to limit the scope of the *ComSeC Scheme* 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. We request DoT to exempt products like LAN switches, 2-wired telephones equipment,

PABX, etc. which are used inside a customer data centre/campus environment for intra-communication in the free band spectrum.

2. **Burden of multiple testing and certification:** At present, in order to place certain wireless products like Access Point, LAN Switch, Router, Mobile phones, etc., in the Indian market, the OEMs are required to obtain (a) WPC certificate from the WPC wing of DoT, (b) MTCTE certificate from the TEC wing of DoT and (c) *ComSeC* from the NCCS wing of DoT. In addition to the above, for certain products like Mobile phones and Servers (which are intended to be covered under the future phases of MTCTE) are already covered under the MeitY's Compulsory Registration Order (CRO) and are required to be tested and certified with BIS.

   In all the above certification scheme, there are some overlap in the testing standards and certification requirements and is a replication of efforts for all OEMs. Such multiple testing and certification scheme not only increase the costs, time and efforts of the OEMs, but also negatively impacts the ease of doing business in India.

   Industry Request: We request DoT to carry out a study to identify products which are governed by multiple divisions in a ministry and multiple ministries for the same product. There should be a single consolidated scheme for testing and regulatory certification, rather than making the OEMs visit multiple labs and multiple agencies (like WPC, TEC, BIS and NCCS) for getting the testing and certification done. Please consider a single-window clearance for all product certifications through one platform with defined TAT (Turn Around Time) with one control point of governance within a single Regulatory Organisation similar to FCC/EU/OFCOM/ACMA or any other ICT regulator in other parts of the world. There should be one application/registration fee, one testing fee, one renewal fee, one recertification fee and most of all, one control point of governance.

   We request the DoT and MeitY to carry out a joint study to identify the products which are currently covered under the CRO and MTCTE scheme. The products should be ideally governed under one regulation which ensure complete testing and certification of the product.

3. **Lack of testing ecosystem:** Though India has mandated in-country testing of telecom products, there are limited testing labs. As of the government sources, there is only one lab for security testing across the country. The requirement of multiple testing schemes like MTCTE and *ComSec* places multiplier cost effects on the OEMs/ importers. The procedure requires each OEM to either (i) ship multiple samples of equipment to the various labs, thus increasing the cost of the overall testing OR (ii) get the testing done sequentially in the labs, thereby increasing the testing duration and running the risk of equipment damage during lab transfers and destructive testing.

   Industry Request: We request DoT to not mandate the security requirement testing and certification until the testing ecosystem with sufficient labs are established in India. Industry believes until the total duration for complete product testing and certification is reduced to 8 to 10 weeks, the certification scheme should not be enforced.

4. **Non-compliable requirements of Indian Telecom Security Assurance requirements (ITSARs):** The way the ITSAR documents are developed today, they are not in a state to be interpreted directly as test cases. Many of the requirements in ITSARs ask for disabling of options in the product at the product development stage; however, products are not manufactured or developed for a specific country (India for example) but are built with a wide range of features for the global market. However, based on the ITSARs the telecom operator can configure the product to exactly to meet the ITSAR specifications and ensure that the needs of ITSARs are fully met. Similarly, the ITSAR requires re-testing for every software update/ patch/ bug fix. With the fast development in the technological world, there are frequent updates released

by the software firm to keep the customers abreast with the developments. In some product categories like Mobile phone and CPE (like Routers) the software updates are as frequent as on a monthly basis. In such cases, it is extremely difficult to continue testing the products. Moreover, going by the normal security testing and certification time as defined in the *ComSeC Scheme*, it would take a minimum 6 months to get the *ComSeC* Certificate. By then, many a time, the technology would become obsolete. Again, source code review/analysis is mentioned in the ITSAR documents (for example you may kindly refer to the ITSAR Draft for Mobiles Section 6.17 namely Vulnerability Testing Requirements published by NCCS). The source code constitutes commercially valuable, confidential and sensitive information.

Industry Request:

- ITSARs are recommended to be stated in a way that they are clear and definite, and the Requirements are testable. It should not be a statement of intent or a desired state without exact result described.
- 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 product releases.
- With the fast development in the technological world, it is important that the security requirements also keep up with the pace. This can be ensured by having regular stakeholder engagement with industry and utilizing their expertise in developing the latest standards.
- Legal security measures are already in place under the Information Technology Act, 2000 and given that the source code constitutes confidential and sensitive information, we would request DoT to remove this requirement from the ITSARs, wherever applicable currently.

  .

5. **Requirement of presence of Validator during security testing**: We believe the requirement of performing the security testing in the presence of a validator would only delay the testing process, as the testing would depend upon the availability of the validator.

   Industry Request: We request the requirement testing in the presence of a validator be dropped from the *ComSec Scheme*.

The ICT industry firmly appeals to the DOT to look into the above-emphasized practical issues which will impede the ease of doing business in the country under such a parallel certification scheme.

As the industry body, we will continue to advocate on such concerns and anticipate for a suitable action to be taken at the earliest in light of the magnitude of the above issue.

With regards,

George Paul
Chief Executive Officer

CC: Shri Bharat Kumar Jog, Member-Services, Department of Telecommunications
CC: Shri Udai K Srivastava, Sr. DDG - TEC, Department of Telecommunications
CC: Smt. C V L Naga Leela, Sr. DDG – NCCS, Department of Telecommunications