Annexure-I

Issues with these new regulations:

1. Escrow of all source code – with full powers to the authorities to open and access the proprietary technology with very open release conditions. This tantamount to complete surrendering of IPR and transfer of technology.

2. Unlimited Liability of the vendors

3. These regulations have been drafted towards a complete/managed services environment and would be impractical for box or parts suppliers.

4. Bound by current and future regulations

5. The document makes reference to Common Criteria labs. The agreement, however, is not clear about how the Common Criteria is used and fits-in the structure of the agreement.

General Comments:

A1. Since this agreement is supposed to be a private contract between the Telecom Service Provider (TSP) and Vendor of the equipment/product/service, the relationship between TSP and Vendor varies depending upon scope, price and the nature of products. An agreement of this nature is seriously detrimental to trade and commerce and impacts fair play and action. A standard template will disadvantage the vendor in discussions with TSP and hence is not conducive to trade and business. This will lead to unfair trade practice and is against the basic principles of fair trade under the WTO. The document in many places seems impractical to implement and not business friendly.

~~A1.~~A2. From a national perspective, the security of the network should be the responsibility of the TSP and they should be made liable by the Government for any breach. In turn, the TSP should bind the vendor of core equipment to use the international standard, the Common Criteria, for independent certification of the assurance of the produc. This important and critical part is missing from the document. The document makes reference to Common Criteria labs. Common Criteria is the accepted international standard for certifying product assurance for hardware and software products. The agreement, however, is quite unclear about how the Common Criteria is used and fits-in the structure of the agreement. There are multiple tests for equipment running throughout the document. We suggest Government should accept a Common Criteria certification, by any one of the labs listed at the end of the document, as the single and only requirement for products pursuant to the agreement. Further, the July 28th regulation appears to indicate that the vendor can not use a Common Criteria certification issued by an independent

Formatted: Bullets and Numbering

lab that is situated in the same country as the vendor – this is unworkable, fractures the underlying Common Criteria Recognition Argeement ("CCRA") (which India is a signatory to) structure of mutual recognition, and should be deleted. The CCRA is based on any CCRA member country accepting the certification of these, chosen, validated, audited, certified, independent labs -- a key concept is that these few CC-worthy labs, are certified by the limited number of CCRA certificate issuing countries (14 countries) to be worthy of issuing CC certifications. And these labs are independent of any government.

A3. As a general matter, this draft template of the agreement seems to be drafted from the perspective that the Vendor will be or effectively will be managing the entire network. Mostly that is not the case.

A4. In some cases the services which are being provided by Vendor to the TSP is insignificant in quantum or is not a very sensitive service which necessitates this procedure and hence this Agreement template is bound to cause confusion and commercial inevitability apart from interpretational issues on account of vagueness. As per this document terms are being stipulated on Vendor's of the TSP.

~~A4.~~A5. The information which needs to be protected or be covered under scope of this Agreement is very broad. Some of the information of TSP may not necessitate handling under such detailed processes and security regime. The relevance of this document to supplier of a product or software is not clear. Most of the terms of this agreement can be mutually discussed between Vendor and TSP as part of the security policy.

Formatted: Bullets and Numbering

~~A4.~~A6. In most cases, all vendors do not provide the entire network equipment and services such as installation and maintenance services. As such, there are many detailed procedures/requirements included in the draft template that would not be applicable to such vendors who provide only specific parts of the network. If these smaller vendors have to sign this kind of an agreement, it would be impractical as well as prohibitively expensive to provide. If the DOT insists that ALL vendors sign this same form, this will effectively discriminate smaller vendors or vendors who are generally providing only equipment and simple services. Ideally, the DOT should let the TSP and the Vendor negotiate what security procedures should apply corresponding to the actual agreement/services that are being provided.

B. General Comments on key issues

B1. Source Code escrow: Mandatory requirement of providing source code is unprecedented and not in conformance with international norms. A vendor will not be able to provide source code due to the following reasons

a. Source code is the core IPR of the vendor worth several billions of dollars and at the core of the business value; by providing source code in escrow there is a huge risk of compromise of IPR

~~a.~~b. There is no precedence of world class reputed vendors providing source code to the Governments on National security consideration. India would set an unhealthy precedent of making such a mandate. The integrity of the source code enhances its security. On the other hand if the Government's around the world mandate escrow of source code with very loose release conditions as is being attempted by this template agreement, and if the vendors there is a serious risk of source code being compromised and getting into the hands of undesirable players. Increasing risk of spyware and malware

~~a.~~c. Technology vendors do not have full ownership of the IPR of the technology that they sell and hence do not have the capacity or the legal rights to put the designs and the software in an escrow account

~~a.~~d. A service providers around the world including national carriers do not seek source code in escrow account with Government even on commercial terms for the following reasons:

i. It will not enhance his security by any measure

~~i.~~ii. There will be millions of lines of code which will be practically difficult to comprehend

~~i.~~iii. It will be commercially very expensive

B2. Regulatory Matters. Sweeping provision binding vendors to all present and future regulatory compliance of the TSP in performance of the contract; no right to decline to fulfil should regulation change.

~~B2.~~B3. Limitation of liability. Effectively, under this draft, the vendor would have unlimited liability. More importantly, this draft requires a vendor to indemnify all amounts/losses/damages imposed on the TSP by the Indian government.

~~B2.~~B4. Confidentiality - It is too wide. . Confidential Information needs to be defined strictly and exceptions to confidentiality to include release pursuant to a Court order.

~~B2.~~B5. Termination/Breach - every breach is termed as Material breach. There needs to be some breaches which are not material and can be cured.

~~B2.~~B6. Security related tests - No definitive/exhaustive list given. This gives the liberty to enlarge the purview of tests at any time

Detailed comments on the template:

1. Page 4 texts – It is stipulated that in case of any conflict, the condition of this agreement shall prevail. This condition restricts Vendor's right during negotiations

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

while entering into new contracts with the Operator which varies and differs in its own nature subjective to the type of supplies and contractual obligations e.g.. Network equipment only, IT equipment only, Managed Services and only box supplies with standard warranty etc.

2. Clause 4.6.1 – The requirement under this clause is to ensure that by means of tools, resources etc. the services of the TSP remain operational at all times as per QoS parameters laid by the TRAI. We believe this condition should only be applicable during a Managed Services contract and not to be an obligation on the Vendor under a simple box supply contract.

3. Clause 4.7.5 – This clause mentions software build including upgrades. The Vendor cannot be forced to provide such upgrades etc. free of cost. Further, if the Operator fails to buy upgrades or does not have an AMC, any liability of leakage of Sensitive Information should be that of the Operator. It should be subjected to contractual obligation and the scope of work agreed under a contract.

4. Clause 4.7.8 & 4.7.10 – These clauses enumerate that the entire responsibility and obligation relating to security is on the Vendor. This should be a shared responsibility and obligation.

5. Clause 4.7.12 – The last sentence in this clause (Vendor shall continue its service without any interruption in the event TSP does not agree to Vendor concern) is requested to be deleted as it allows no discretion or option to the Vendor and fair play between the parties.

6. Clauses in Section 7 - The document makes reference to Common Criteria labs. Common Criteria is the accepted international standard for certifying product assurance for hardware and software products. The agreement however is quite unclear about how the Common Criteria is used and fits-in the structure of the agreement. There are multiple tests for equipment running throughout the document. We suggest that Government should accept a Common Criteria certification, by any one of the labs listed at the end of the document, as the single and only requirement for products pursuant to the agreement.

7. Clause 7.12 – We believe and request that the Escrowing of source code requirement be exempted/deleted from the agreement and Vendor must not be compelled to provide any such information/material for few important reasons highlighted below:

    a. It is Vendor’s proprietary information and an asset of the company (Intellectual Property).

    b. Escrowing of Source code is unprecedented as an international business practice.

    c. Self certification submitted to Operators and in-turn to your office by operator aligning directive issued vide letter 10-15/2009-AS-III/ dated 18th March 2010, having a provision of huge penalty in our view provides adequate safeguard in respect of our national security interest.

d. Vendors are not owners of the complete IPR of the technology being sold by them and hence are not in a position to put the designs and software in an escrow.

8. Clause 8.8 & 8.9 – Conditions imposed under this clause are only against the Vendor which if breached would tantamount to material breach and the Vendor is required to indemnify the TSP. It may be noted that this should be reciprocal. Regardless of the foregoing, it is being presumed that the Vendor would have the right to take remedial measures upon service of a notice. In addition, the alleged breach by the Vendor should be solely and directly attributable to the Vendor and it should be subject to a legal recourse. The damages/claims against the Vendor should be subject to a maximum of overall cap on limitation of liability.

9. Clause 9.2 (a) and 9.2 (f) – Under these clauses, the Vendor is required to comply with all regulatory matters without limitation and at its own cost. While we agree with the spirit but the entire burden, liability, responsibility, obligation etc. must not be passed on by the TSP to the Vendor. All such requirements need to be discussed and mutually agreed between the parties. Also the Vendor cannot be expected to give access rights of its premises to the TSP anytime and without prior intimation. TSP cannot be allowed to enter the premises of the Vendor at its own discretion. However, Vendor can facilitate any investigation or enquiry.

10. Clause 15 – Limitation of liability clause should be mutual and there must be an overall cap on liability. Further, this clause carves out an exception to indirect and consequential damages only and should include in the exceptions - special, incidental, remote damages, loss of profit, loss of data, loss of revenue etc. Moreover, the Sub clause (II) is completely unfair to the Vendor and the Vendor must not be compelled to accept it as it stands. We also believe overall liability must be capped and must not be subjected to every purchase order/procurement.

11. Clause 16 Para 1 & 2 – Termination rights should be mutual between TSP and Vendor. Further, if the Agreement is terminated for any reason, the TSP retains the right to terminate the other supply/services agreement as stated in Para 2 of the said clause. This gives no recourse to the Vendor. As the conditions of breach is one sided and in favor of the TSP, we request you to kindly consider amending the clause appropriately.

12. Clause 16 Para 3 – Under this clause the Vendor is required at its own cost and expense to take all steps to restore the lost or corrupted information of the TSP. Please note that such obligation may be placed on the Vendor provided the Vendor has control over the TSP information through a managed services contract and the Vendor cannot be liable for the same under a simple supply contract.

13. Force Majeure clause has not been included. We request you to kindly include a clause on Force Majeure for various situations like Terrorist attack, any war or hostility, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts and any other unavoidable act of God.

14. Further, many other clauses such as 3, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.2.4, 4.2.6, 4.2.7, 4.3.2, 4.3.3 3rd bullet, 4.4.4, 4.6.2, 4.7.1, 4.7.2, 4.7.3, 4.7.14,7.1 to 7.11, 5.3, 5.4, 6.1 (k), 6.1 (m), 6.1 (p), 6.1 (q), 6.1 (s), 6.1 (t), 9.2 (b), 9.2 (e), 12 (c), have cost implications directly and solely referable to the Vendor, which in our view should be mutually agreed between TSP and Vendor and work out ways to minimize such costs for the benefit of the industry, consumers and the country. Our overall submission is that these obligations required to be fulfilled by the vendors should be subject to mutual discussions and understanding in line with the objectives of national security while also following good business practices.

15. Also there are many clauses which require further clarification and understanding such as Clause 4.1.2, 4.2.11, 4.4.5, 4.7.6, 4.7.7, Notes Page 21 and 22, 5.2 (d) 6.1 (p), 6.1 (x), 6.2, 9.2 (d), 10, 10.5, 8.6 (d) , 8.7 (a), 8.7 (b) , 8.8, 8.10, 12 (a), 12 (b), 13, 14, 14.4 with operator and your office.
