Telecom Hotline

June 28, 2011

IMPORTANT SECURITY-RELATED AMENDMENTS TO TELECOM LICENSES

Over the past year and a half, the Indian telecom sector has witnessed much tumult over issues of security with the Department of Telecommunications, Government of India ("**DoT**"). The DoT has issued various notifications that impose onerous obligations and restrictions particularly with respect to foreign telecom vendors (collectively referred as "**Prior Notifications**") [1]. These Prior Notifications created a lot of uncertainly in the industry both within the vendor community and among the telecom licensees as to the scope and ambit of the requirements.

The DoT recently announced that all Prior Notifications are to be superseded by amendments to the telecom licenses themselves [2] ("**Amendment**"). In this hotline, we offer our quick analyses of the Amendment.

ANALYSIS OF THE SALIENT FEATURES OF THE AMENDMENT

- **Certification and Internal Security Policy:**

  All telecom licensees are required to ensure that all network elements be tested in Indian laboratories commencing from April 1, 2013; till such date, the telecom licensees are free to use any certifying agency of their choice. The DoT is to provide an illustrative list of certain certified agencies on their website.. Further the telecom licensees also have to conduct a yearly audit on their networks (the first audit to be completed before May 31, 2012). In addition:

  - The telecom licensee is obligated to (i) maintain relevant security standards while procuring the telecom equipment, and (ii) a list of features, equipments, software, which list must be open to inspection at the discretion of DoT (iii) create facilities for intrusion detection and monitoring by May 31, 2012.
  - Only Indian residents shall be eligible to be employed as key officers [3].
  - Telecom licensee has been obligated to maintain a record of operation and maintenance procedures, not limited to, operation and maintenance command log, user-ids; software updates and changes and supplier chain.

  Analysis:

  This requirement is in line with the intent of certain requirements that were imposed by the Prior Notifications. It is pertinent to note that in the Prior Notification, the DoT had made a distinction between "*core*" and "*passive equipment*", where only core equipment was required to undergo security clearance. However, the current Amendment does not provide such distinction, nor does it clarify which elements of the telecom network need to be audited. As such the scope of the audit is apparently very broad. Further, in light of the fact that the security standards to be followed are international standards, mandating testing to be performed only by Indian laboratories may not be necessary and may pose impediments to the efficiency of the entire process and raises a number of intellectual property and confidentiality concerns.

- **Inspection:**

  The telecom licensees must ensure that their vendor agreements with their vendors contain provisions enabling the , the telecom licensee and/or DoT (or its agencies) to inspect the hardware/software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check at any during the supply of telecom equipment by the vendors. Such inspection shall be limited to two per Purchase Order under the vendor agreements. Where the relevant purchase order value if more than INR 50 crores and the duration of such visits exceeds 40 man days per visits, the costs shall be borne by the telecom licensee or can be passed on to the vendors.

  The Amendment also lists out the contours of the provisions which may be incorporated into the agreement to be executed between the telecom licensee and the vendor so that the vendor supplied equipment is “safe to connect” in the network. The DoT has stated that they shall make available a template agreement with suggested clauses which the telecom licensees and vendors may use as a base template.

  Analysis:

  This provision appears to be quite onerous and invasive.

  - As emphasized above, the likelihood of manufacturing facilities and supply chain stretching across multiple geographies is very high. While the DoT’s mandate of being allowed to inspect all stages and components of a supply chain (including the actual manufacturing facilities) may be agreed contractually with the telecom licensee and the vendor, in spirit this requirement is akin to the DoT assuming extra-territorial jurisdiction which it and the telecom licensee may not be able to enforce. Further, in any event, the local regulatory environment of such geographies may not permit such interference by a foreign regulator which in turn may

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Audio

Securities Market Regulator’s Continued Quest Against “Unfiltered” Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

“Investment return is not enough” Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI’s Consultation Paper on Simplification of registration for FPIs

defeat the implementation of this provision. The Vendor will generally be bound by strict confidentiality provisions with its suppliers and manufacturers and it will be impossible for them to agree to such provisions without committing a breach of their confidentiality obligations.

- Since the Amendment does not provide any specific instances which would trigger the DoT's inspection rights, it could be interpreted that the DoT has an unfettered right of inspection irrespective of any actual cause or reason to believe that a security breach has occurred or is threatened.
- The Amendment does not specify the manner in which the inspection costs are to be borne for purchase orders whose value is less than INR 50 crores or where the inspection duration is less than 40 man days.
- While the DoT has said that they will make available a template agreement, it is not clear whether the DoT is actually referring to the infamous Security and Business Continuity Agreement Template which was approved and circulated by the DoT on July 28, 2010 ("**Template Agreement**"). This template agreement contained draconian provisions relating to mandatory transfer of technology, intellectual property and escrow. It should also be noted that while the telecom licensees are free to "add, modify or delete" provisions of this template, it is more likely that the telecom licensees will take a safe stand and ensure that all the stringent provisions are included in their agreements with the vendors.
- In our view the certification requirements in the Amendment (which we discussed in point 1 above) should suffice and DoT will be able to proceed against the TSP or the Vendor if there is any breach. There is no need for the DoT to intrude into the supply chain and manufacturing facilities.

- **Penalties:**
  - **Monetary:** The Amendment has attempted to differentiate between an intentional breach and an inadvertent breach.
    - Penalty of up to INR 50 crores has been prescribed for any security breach caused due to inadvertent inadequacy ("**Inadvertent Breach**"). The DOT shall set up a five member panel which will determine whether the breach is due to such inadvertent inadequacy and the amount of penalty.
    - Penalty of INR 50 crores has been prescribed for any intentional omissions / deliberate vulnerability or deliberate attempt for security breach ("**Intentional Breach**").
  - **Cancellation and Blacklisting:**

    In addition to the monetary liabilities on the telecom licensees, the DoT may also cancel the license of the telecom licensee as well as blacklist any vendor/supplier of telecom equipment from doing business in India. The DoT has mandated the insertion of a clause to allow DoT, the discretion to blacklist such vendor/supplier in all equipment procurement agreements entered into by the telecom licensee.

Analysis:

Although the DoT has attempted a differentiation between an Intentional Breach and an Inadvertent Breach, they have not defined what would be deemed to be an "inadvertent inadequacy". The telecom licensee or the Vendor have not been provided the right to any due process or appeal from the decision of the DoT committee. This is against the principles of natural justice.

The Amendment does not prescribe any procedure which is to be followed in the determination of an Intentional Breach. It is also unclear whether the DoT committee (which determines events of Inadvertent Breach) would determine events of Intentional Breach. Further, since Intentional Breach implies a higher degree of culpability on the telecom licensee and/or the Vendor, it is surprising that the DoT has not prescribed any adequate due process to be followed in determining such liability.

The provisions pertaining to blacklisting are perhaps the most draconian. The DoT has assumed absolute power to discredit the vendors/suppliers without following the principles of natural justice. However, it is unclear what "blacklisting" means. Various interpretations could arise, e.g.: (i) the vendor not being able to carry any further business in India (this could be time bound of perpetual); (ii) the vendor not being able to supply only those products which caused the security breach; (iii) the vendor not being able to supply products for a particular territory etc.

In our view, apart from clarifying the various ambiguities in the Amendment with respect to intentional and inadvertent breach, the DoT must ensure a transparent due process in determining whether any breach has been committed.

CONCLUSION

The telecom industry has been waiting for clarifications from the government on Prior Notifications. The aim of the Government in implementing the Amendment is to address the concerns of the industry arising out of the Prior Notifications and address security concerns connected with this industry.

Under the provisions of the Prior Notification, the telecom vendors and telecom licensees had in some instances executed documentation in which they had incorporated the provisions of the Prior Notification including the Template Agreement. Since this Template Agreement appears to have been superseded, the stakeholders must re-look at their purchase orders and documentation and determine whether the supersession would automatically nullify their obligations or they would need to enter into new agreement to amend their obligations.

In addition, it should be remembered that at the time when the Prior Notifications were in force, some of the vendors had provided self certification documentation which was basically in the form of back to back obligations with respect to the obligations under the Prior Notifications. The fate of these self certifications is not clear in that whether the supersession of the Prior Notification implies that such self certifications are cancelled or if these certifications continue in a parallel dimension. While the Government has certainly attempted to address the concerns of the industry over security issues, there are certain issues where further dialogue and clarification would be required.

– Telecom Practice Group
You can direct your queries or comments to the authors

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024

[1] Please refer to our hotline at http://www.nishithdesai.com/...HOTLINE_Aug0410.htm and the article published athttp://www.nishithdesai.com/Media_Article/2010/India's...Requirements.pdf wherein we have analysed in detail the various requirements imposed by the DoT

[2] (i) Letter No. 10-15/2011-AS.III/(21) dated May 31, 2011 which amends the UAS License; (ii) Letter No. 10-15/2011-AS.III/(22) dated May 31, 2011 which amends the Basic Service License Agreement; (iii) Letter No. 10-15/2011-as.III/(23) dated May 31, 2011 which amends the CMTS License.

[3] Chief Technical Officers, Chief Information Security Officer, Nodal Executive and System Administrators