Government of India
Ministry of Communications & IT
Department of Telecommunications
(DS Cell)

No. 815-66/2011-DS **Dated:03.06.2011**

To

All Commercial VSAT Licensees migrated to NTP 99

Subject: Amendment to the Commercial CUG VSAT Licence Agreement for security related concerns for expansion of Telecom Services in various zones of the country

Due to Security related concerns terms & conditions of Commercial CUG VSAT Licence were amended vide letters No. 824-725/2005-VAS/Vol.III dated 15th December 2009 and 25th August 2010.

In super-session of these amendments and in exercise of the power vested in the Licensor under clause No. 12(ii) of Commercial CUG VSAT Licence Agreement, inter-alia, reserving the right to modify at any time the terms and conditions of the Licence in the interest of national security and public interest or for the proper provision of TELEGRAPH, the Licensor hereby inserts, with immediate effect, the following clause in the said Licence, namely;

"1.1A (i) The Licensee shall be completely and totally responsible for security of their networks. They shall have organizational policy on security and security management of their networks. **Network forensics, Network Hardening, Network penetration test, Risk assessment, Actions to fix problems and to prevent such problems from reoccurring etc** should be part of the policy and they should take all measures in respect of these activities. They should submit their policy to Licensor within 30 working days from the date of this amendment for record.

ii) In furtherance of organizational security policy, the Licensees shall audit their network or get the network audited from security point of view once a year from a network audit and certification agency. The first audit of the network should be completed within 12 months of the issue of this amendment and thereafter once in a financial year. A list of some of the agencies which might carry out network audit from security point of view will be on the website of DoT. The list is purely for information dissemination as a facilitating measure and TSPs are free to engage the service of any other agency for this purpose, which is certified to carry out

03/6/2011

the audit as per ISO 15408 and ISO 27001 standards, because network security is their responsibility.

iii) The licensee shall induct only those network elements into his telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, Telecom and Telecom related elements against 3GPP security standards, 3GPP2 security standards etc from any international agency/ labs of the standards e.g. Common Criteria Labs in case of ISO/IEC 15408 standards until 31st March 2013. From 1st April 2013 the certification shall be got done only from authorized and certified agencies/labs in India. The copies of test results and test certificates shall be kept by the licensee for a period of 10 years from the date of procurement of equipment.

iv) The Licensee shall include all contemporary security related features and features related to communication security as prescribed under relevant security standards while procuring the equipment and implement all such contemporary features into the network. A list of features, equipments, software etc procured and implemented shall be kept by the licensee till they are in use, which may be subjected to inspection and testing by the Licensor at any time, in the network or otherwise, at the option of the Licensor.

v) The licensee shall employ only Resident, trained Indian Nationals as Chief Technical Officer/s, Chief Information Security Officer, Nodal Executives for handling interception and monitoring cases and incharge of network elements like Hub, NMS, Switches, Central Database etc. and System Administrator/s.

(vi) The Licensee shall

a. Ensure that all the documentation, including software details are obtained from manufacturer/vendor/supplier in English language.
b. Keep a record of operation and maintenance procedure in the form of a manual.
c. Keep a record of all the operation and maintenance command logs for a period of 12 months, which should include the actual command given, who gave the command, when was it given with date and time and from where. For next 24 months the same information shall be stored/retained in a non-online mode. For this purpose licensee shall keep a list of User ID linked with name and other details of the user duly certified by the system administrator. The user list shall be provided to licensor or agencies designated by the Licensor as and when required.

03/6/2011

d. Keep a record of all the software updations and changes. The major updation and changes should also be informed to licensor within 15 days of completion of such updation and changes.

e. Keep a record of supply chain of the products (hardware/software). This should be taken from the manufacturer/vendor/supplier at the time of procurement of the products.

f. Comply with the conditions of Remote Access (RA).

(vii) The Licensee shall create facilities for monitoring all intrusions, attacks and frauds and report the same to the Licensor and to CERT-IN. Such facilities shall be created by the Licensee within 12 months of issue of this amendment and be reported to Licensor as and when created during this period.

(viii) The licensee through suitable agreement clauses with vendor shall ensure that the Vendor/Supplier allow the Telecom Service Provider, Licensor/DoT and/or its designated agencies to inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check any time during the supplies of equipment. The number of such visits will be limited to two in a Purchase Order. The expenditure for such visits for order valuing more than Rs 50 crore upto 40 man-days per visit shall be borne by the licensee directly or through vendor.

(ix) a) A penalty upto Rs 50 crores will be levied for any security breach which has been caused due to inadvertent inadequacy/inadequacies in precaution on the part of licensee prescribed under this amendment. Licensor shall constitute a five members committee, which shall include two cyber security experts, to determine whether the breach is due to inadvertent inadequacy/inadequacies or otherwise. The committee shall also decide the amount of penalty depending upon loss, gravity of breach etc.

b) In case of inadequate measures prescribed under this amendment, act of intentional omissions, deliberate vulnerability left into the equipment or in case of deliberate attempt for a security breach, penalty amount will be Rs. 50 crores per breach. The same breach in the same equipment purchased through same PO or in the same lot or the same negligence at the same time at multiple locations in an operator's network will be considered as a single breach for the purpose of levying penalty under this clause. The Licensee shall deposit the penalty amount with the Licensor within 30 days of the issue of Notice.

c) Besides the penalty, liability and criminal proceedings under the relevant provisions of various Acts such as Indian Telegraph Act, Information Technology Act, Indian Penal Code (IPC), Criminal Procedure Code (Cr PC) etc can be initiated. In such cases licence of

03/6/2011

the licensee can also be cancelled, vendor or supplier who supplied the hardware/software, that caused the security breach, could be blacklisted for doing business in the country or both. The licensee must include the clause of licensor discretion of blacklisting of vendor or supplier in such cases in the agreement signed with vendors/suppliers.

03/6/2011

(Vishal Kumar)
ADG(LR)
Tel: 23710248

Note: Some other suggested steps, which help in increasing the security of the telecom network, are given in Annexure to this letter. Govt. may, however, make any of these suggestions mandatory whenever it feels it necessary to do so.

Copy to:

1. Secretary TRAI, New Delhi
2. Wireless Advisor, WPC wing, New Delhi
3. Sr DDG (WPF), DoT, New Delhi
4. DDG (Security)/DDG(CS)/DDG(AS)/DDG(LF)/DDG(Security-TERM), DoT
5. JS(IS), MHA
6. DDG(C&A), DoT, New Delhi for publishing on the DoT website
7. Respective License Agreement files.

Annexure to letter No. 815-66/2011-DS Dated:03.06.2011

Some suggested steps, which help in increasing the security of the telecom networks are:

a) May sign a suitable agreement with hardware/software manufacturer/vendors and/or suppliers of services to ensure that the equipment/services/software they supply are 'Safe to Connect' in the network, have been checked thoroughly for risks and vulnerabilities, all addressable vulnerabilities have been addressed, non-addressable vulnerabilities have been listed with remedial measures and precautions provided. The agreement should cover aspects related to security measures like access control, Password control and management etc. Clauses addressing the service continuity and service upgradation should also be suitably included in the agreement, with consequences defined for each party in case of breach, particularly the security breaches. As an information dissemination and facilitating measure, suggested clauses for such an agreement in the form of a template will be available on the website of DoT. The service providers may take all or selected provisions from this template, depending upon the type of services they avail from a vendor/supplier. They are free to add, modify, delete any of the clauses from this template, because security of their network is their responsibility and they will be liable for any security breach.

b) The Licensees should endeavour to create a forum, say, Telecom Security Council of India (TSCI), on a voluntary basis to increase the security assurance levels and share common issues.

c) The Licensee shall build their own capability and capacity to maintain and operate the network, preferably through local maintenance personnel, because the telecom network is a security sensitive infrastructure.

03/6/2011