RECOMMENEDED CLAUSES IN THE FORM OF A TEMPLATE FOR THE AGREEMENT BETWEEN TELECOM SERVICE PROVIDER AND THE VENDOR OF EQUIPMENT, PRODUCTS AND SERVICES FOR ADDRESSING SECURITY CONCERNS

Note:

(i) The clauses listed in the template are applicable for a comprehensive service agreement which include supply, installation, commissioning, maintenance and operation and services. Since TSP enter into agreements with vendor/ suppliers in various colours and shades covering different aspects of supply and services they can pick up the clauses relevant to the type of agreement they are entering into with their supplier/ vendor or could reword them, including the definition of terms so as to suit their requirements.

(ii) Picking up the clauses from this template partly or fully does not absolve the licensee of its obligation to ensure the security of its network and communication, which is solely their responsibility.

Terms and Conditions

(i) With a view to help and address the business continuity, communication, security and security management of TSP's networks in respect of equipments / products/ software / services, the parties hereto are desirous of recording the terms and conditions as set forth in this Agreement.

(ii) This Agreement would be read in conjunction with the respective contractual agreements the TSP and the Vendor, which they have for the supply of Equipments/Products and Services. In case of any conflict, the conditions of this agreement shall prevail.

1. Definition of Terms and expressions

Unless the context otherwise requires, the different terms and expression used shall have the meaning assigned to them for the purpose of this agreement in the following paragraphs:

a. **"Access"** - interconnection with TSP Systems or access to or use of TSP Information stored on TSP Systems through interconnection with TSP Systems or access to or use of TSP Information stored on Vendor Systems or access to or use of TSP Information stored in any mobile device.

b. **"Authorised"** - TSP has approved Access as part of the authorisation process and the Vendor Security Contact has a record of this authorisation. "Authorisation" shall be construed accordingly.

c. **"Commencement Date"** and "End Date" means the date the agreement is executed and the date when the validity or term of this contract ends or terminated.

d. **"Contract Personnel"** means dedicated resources of the Vendor in terms of employees, subcontractors including employees of sub contractors and agents including agent's sub contractors and their employees engaged for the purpose of this Agreement.

e. **"NAIF"** means Network Authorisation and Interconnect Facility is a procedure for registration of global network interconnect between TSPs and external companies.

f. **"Sensitive Information"** means any TSP Information marked as classified as per TSP's data classification policy or deemed business critical. This also includes any other data, or element of information, notified as such by the Government (e.g. IT Act 2000).

g. **"Security Standards"** means all the relevant contemporary standards associated with national and international security standard related to IT & Telecom equipment hardware and software and those related to information & communication security, including but without limitation to ISO 27000 series, ISO/ IEC 15408, 3GPP, 3GPP2, WiMAX etc. and as evolved from time to time.

h. **"Subcontractor"**- any person, partnership or corporation with whom the Vendor places a contract and/or an order for the supply of any equipment, item, service or for any work in relation to the purpose of this Agreement. "Subcontract" shall be construed accordingly.

i. **"Supplies"** means all components, materials, plant, tools, test equipment, documentation, hardware firmware, Software, spares parts, services and all the things & items to be provided to TSP pursuant to the Agreement together with all Information and Work the Agreement requires to be supplied or performed for TSP.

j. **"Term"** means the term of this Agreement from the [Commencement Date] to [End Date].

k. **"TSP"** means Telecom Service Provider licensed under section 4 of Indian Telegraph Act 1885 by the Licensor, Government of India

l. **"TSP Group Security"** means the security organisation based within the TSP Group Company.

m. **"TSP Information"** means all data including data, text, image, sound, voice, codes, circuit diagrams, core & applications software and database, intellectual property as well as personal, public, operational and services data in TSPs custody which is and /or received which are supplied/ shared with Vendor for the purpose of this Agreement or are obtained by the Vendor on behalf of TSP.

n. **"TSP Items"** - all items provided by TSP to the Vendor and all items held by the Vendor which belong to TSP.

o. **"TSP Regulatory Contact"** means incharge of TSP Regulatory Operations or such other person whose details shall be notified by TSP to the Vendor from time to time.

p. **"TSP Security Contact"** means incharge of TSP Security Operations Centre or such other person whose details shall be notified by TSP to the Vendor from time to time.

q. **"TSP Systems"** means any TSP computer, application, databases , network infrastructure, network elements and appliances, core and applications software or such other systems as may be agreed in writing from time to time between TSP and the Vendor.

r. **"Vendor"** means who supplies Equipment, Software and/or managed services to TSP for the purpose of installation, provision, operations and/or maintenance of TSP's networks.

s. **"Vendor Security Contact"** means such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

t. **"Vendor Regulatory Contact"** means such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

u. **"Vendor Systems"** means any Vendor owned computer hardware or software, application database or network elements / appliance or such other systems as may be agreed in writing from time to time by TSP and the Vendor.

2. Scope

This Agreement sets out the provisions under which the Vendor will be able to supply equipments and services and be granted Access to TSP Systems, network, equipments, data and facilities and TSP Information including Sensitive Information for the purpose of installation, provision, operations and maintenance by the Vendor

3. International Security Standard Certification

The Vendor shall have contemporary relevant Security standard certification and shall comply with the provisions of security standards certification w.r.t. Telecom & IT equipment hardware and software and those related to information & communication security management, such as ISO 15408 standards as applicable to IT and IT related products, ISO 27001 for Information Security Management System, standards used by other relevant standard formulation bodies for Telecom equipment like 3GPP, 3GPP2, ITU standard etc or equivalent acceptable international standards or certification.

4. **Security Requirements:** The vendor shall comply with following security policies:

4.1 GENERAL

4.1.1 The Vendor shall be Authorised to access only TSP Systems and Informations in accordance with the provisions of this Agreement and only during the term of this Agreement.

4.1.2 The Vendor shall identify to TSP details of Vendor Security Contact at the Commencement Date who will act as a single point of contact for TSP, such as a senior manager or CIO responsible for security, for any security issues. This responsibility shall be detailed within his/her job description. This does not mean that the Vendor shall not be responsible as an organization or company and its management. The vendor security contact shall only be a security cleared Indian national. The security clearance for the security contact will be applied and obtained by the TSP from the Licensor.

4.1.3 As part of the Authorisation process, details of Vendor's Contract Personnel that need Access will be requested by TSP. The Vendor Security Contact shall at all times ensure that only Contract Personnel who have a need to Access in order to fulfill the purpose of this Agreement are Authorised. This authorization and any changes in the personnel would be notified by the Vendor for the information and for the approval (wherever applicable) of the TSP.

4.1.4 Pursuant to Clause 4.1.3 above, the Vendor acknowledges that only the Contract Personnel having requisite training are Authorized to access TSP System.

4.1.5 The Vendor shall have a well defined Information Security policy compliant with ISO/IEC 27001:2005 or have equivalent standards and in line with the TSP's information security policies and requirements.

4.1.6 The Vendor shall ensure that they have information security organization in place to implement the provisions of TSP's information security policies. The Information

Security responsibilities of all Vendor employees working for TSP shall be defined and communicated.

4.1.7 The Vendor shall establish and maintain contacts with special interest groups to ensure that the understanding of the information security environment is current, including updates on security advisories, vulnerabilities and patches and ensure that the same is implemented.

4.1.8 The Vendor shall conduct a Risk Analysis and ensure that all risks due to it own and sub-contractors' operations with TSP are identified, measured and mitigated as per the TSPs requirements. The Risk Assessment report is required to be shared with the Chief Security officer/CISO of TSP.

4.2 PHYSICAL SECURITY

4.2.1 All Contract Personnel including sub contractors and their employees, agents and their employees of the Vendor working on TSP premises shall be in possession of a TSP Identification or Electronic Access Control ("TSP ID/EAC") card. This card is to be used as a means of identity verification on TSP premises at all times and as such the photographic image displayed on the TSP ID/EAC card must be clear and be a true likeness of the Contract Personnel. If the TSP has any advanced identity verification systems the same would also apply. TSP may re-define such verification measures from time to time.

4.2.2 All Contract Personnel including sub contractors and their employees, agents and their employees of the Vendor accessing premises (sites, buildings or internal areas) to fulfil the Purpose, where TSP Information is stored or processed, shall be in possession of an Identification or Electronic Access Control ("ID/EAC") card. This card is to be used as a means of identity verification on these premises at all times and as such the photographic image displayed on the ID/EAC card must be clear and be a true likeness of the Contract Personnel or the Subcontractor or the Vendor's employees, subcontractors and agents. If the TSP has any advanced identity verification systems the same would also apply. TSP may re-define such verification measures from time to time

4.2.3 The Vendor shall not (and, where relevant, shall procure that any Contract Personnel shall not) without the prior written Authorisation of the TSP Security Contact connect any equipment, device or software to any TSP System and where it is not intended to be connected at a point in the TSP system.

4.2.4 The Vendor shall be able to demonstrate that it has procedures to deal with security threats directed against TSP or against a Vendor working on behalf of TSP whilst safeguarding TSP Information.

4.2.5 The vendor and/or its contract personnel shall not access TSP's electronic systems without first obtaining the written consent of the TSP security Contact;

4.2.6 The Vendor's Access to sites, buildings or internal areas where TSP Information is stored or processed, shall be as Authorised and the Vendor and all its Authorised personnel shall adhere to robust processes and procedures to ensure compliance.

4.2.7 The Vendor shall ensure that all TSP Information, Contract Personnel, Vendor Systems and TSP Systems and networks used to fulfill the Purpose are logically and physically

separated in a secure manner from all other information, personnel or networks created or maintained by the Vendor. Additionally, secure areas in Vendor premises (e.g. network communications rooms), shall be segregated and protected by appropriate entry controls to ensure that only authorised Contract Personnel are allowed access to these secure areas. The access made to these areas by any Vendor's personnel shall be audited regularly, and re-authorisation of access rights to these areas must be carried out at least once annually.

4.2.8 The use of digital or conventional cameras, including any form of video camera or mobile phone cameras, of the interior of TSP premises is not permissible without prior Authorisation from the TSP Security Contact. Vendor shall ensure that photography or capture of moving image of Vendor areas where TSP Information is processed or stored shall not capture any TSP Information.

4.2.9 CCTV security systems and their associated recording medium shall be used by the TSP/ Vendor either in response to security incidents, as a security surveillance tool, as a deterrent or as an aid to the possible apprehension of individuals caught in the act of committing a crime. As such, these systems shall be authorised by appropriate TSP Security Contact when used by vendor, and stored images shall be securely held for at least 6 months. Notwithstanding the above, TSP may object to CCTV surveillance if circumstances deem that such surveillance is inappropriate in relation to the purpose of this Agreement.

4.2.10 The Vendor shall maintain a controlled record of all assigned TSP physical assets and assigned TSP Items to them.

4.2.11 The local area surrounding the Vendor's facilities at TSPs premises shall be inspected for risks and threats on a regular basis by the Vendor and such reports made available to TSP.

4.2.12 The Vendor shall disable the Access immediately if any Contract Personnel no longer require Access or change role for any reason whatsoever or whose integrity is suspected or considered doubtful or as may be notified by TSP in accordance with clause 4.3.1.

4.3 LOGICAL SECURITY

4.3.1 The Vendor shall notify TSP immediately if any Contract Personnel no longer requires Access or change role for any reason whatsoever thus enabling TSP to disable or modify the Access rights.

4.3.2 The Vendor shall maintain systems, which detect and record any attempted damage, amendment or unauthorised access to TSP Information.

4.3.3 The Vendor shall, implement agreed as well as generally prevalent security measures across all supplied components and materials including software & Data to ensure safeguard and confidentiality, availability and integrity of TSP Systems and TSP Information. The Vendor shall provide TSP with full documentation in relation to the implementation of logical security in relation to Purpose and shall ensure that it has such security as:

- prevents unauthorised individuals e.g. hackers from gaining Access to TSP Systems; and
- reduces the risk of misuse of TSP Systems or TSP information, which could potentially cause loss of revenue or service (and its Quality) or reputation, breach of security by those individuals who are Authorised to Access it; and
- detects any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained Access and determination of how they obtained it.

4.4 INFORMATION SECURITY

4.4.1 The Vendor shall not use TSP Information for any purpose other than for the purposes for which they were provided to the Vendor by TSP and only to the extent necessary to enable the Vendor to perform as per this Agreement.

4.4.2 The Vendor shall ensure that all information security requirements in this Agreement are communicated including in writing to all Contract Personnel in relation to their role.

4.4.3 The Vendor shall ensure that it operates a proactive strategy to minimise the risk and effects of fraud and other security risks and the Vendor shall maintain processes to monitor such activities.

4.4.4 The Vendor shall ensure procedures and controls are in place to protect the exchange of information through the use of emails, voice, facsimile and video communications facilities.

4.4.5 The Vendor shall use physical and electronic security measures to protect TSP Systems, TSP Information and areas where work is undertaken or where Vendor Systems provide Access.

4.5 CONTRACT PERSONNEL SECURITY

4.5.1 The Vendor shall ensure that the TSP Information provided under this Agreement is used only to the extent necessary to enable the Vendor to perform as per the terms of this Agreement. All Contract Personnel sign a confidentiality agreement either as part of their initial terms and conditions of employment or when they start working in TSP buildings or on TSP Systems and TSP Information. These confidentiality agreements shall be retained by the Vendor and accessible to TSP.

4.5.2 The Vendor shall deal with breaches of security policies and procedures, including interfering with or otherwise compromising security measures, through a formal disciplinary process.

4.5.3 The Vendor shall provide a 'whistleblower' facility, available to all staff, with all TSP related issues reported back to the TSP Security Contact to the extent permissible by the law in a location in India where the Vendor is delivering its Purpose. For the avoidance of doubt, this facility shall be used by the Contract Personnel if TSP's employee, agent or contractor instructs Contract Personnel to act in an inconsistent manner in violation of the Agreement.

4.5.4 The Vendor shall ensure that in respect to any Contract Personnel assigned to this Agreement; it shall carry out recruitment checks in accordance with the provisions in Vendor Pre-Employment Checks Policy defined by TSP.

4.5.5 The Vendor shall ensure that all Contract Personnel maintain a clear-desk and a clear-screen policy to protect TSP Information.

4.5.6 The Vendor shall ensure that an auditable process is developed for the ongoing control and management of Contract Personnel access profiles.

4.5.7 The Vendor shall, and shall procure that any Contract Personnel securely destroy any TSP Information received in a recorded form from TSP (or has recorded received TSP Information), when the Contract Personnel's job or role has changed or terminated.

4.6 SERVICE CONTINUITY ASSURANCE:

Appropriate commercial arrangement should be made by TSP with vendor to assure the continuity of service by including clauses such as:

4.6.1 The Vendor shall ensure by means of all tools, skills, resources that the services of TSP remains operational at all times as per Quality of Service parameters laid down by Telecom Regulatory Authority of India.

4.6.2 At the time of termination of contract or as and when required by the TSP, the vendor shall ensure making over all tools, procedures, documents, softwares, training etc using which TSP system were maintained operated, analyzed, attended etc, by the Vendor so that TSP can continue to provide the services.

4.7 ADDITIONAL SECURITY POLICIES

4.7.1 The Vendor shall have documented operating procedures to discharge the security requirements detailed within this Agreement and provide TSP with access to such documentation in accordance with "Access to Vendor systems" as stipulated in this agreement.

4.7.2 The Vendor shall notify the TSP Security Contact immediately of any changes to its Access method through the firewalls, including the provision of network address translation.

4.7.3 The Vendor shall implement a controlled exit procedure in respect of the individual Contract Personnel to ensure the return of any TSP assets or TSP Items or TSP Information in the possession of the individual when any of the Contract Personnel who have Access, leave the employment of the Vendor or are no longer engaged for the purpose of this Agreement. Such controlled exit procedure shall include a written communication by the Vendor Security Contact to TSP Security Contact of this removal.

4.7.4 The Vendor shall inform the TSP Security Contact immediately upon its becoming aware of any actual or suspected unauthorised Access or misuse of TSP Systems or TSP Information or breach of any of the Vendor's obligations under this Agreement.

4.7.5 The Vendor shall maintain integrity of the software build including upgrades, operating systems and applications from factory to desk. The Vendor shall demonstrate that the software build (both proprietary and off-the-shelf) delivered to TSP is the same as the software build agreed with TSP. The software should not have such bugs, which could hamper security in future including any unauthorized leakage of TSP Information including Sensitive Information.

4.7.6 Self-help systems operated by TSP shall only be remotely accessible by Authorised Contract Personnel.

4.7.7 Any change of location by the Contract Personnel or Vendor for any part of the supply chain or the support centers shall be notified to TSP immediately.

4.7.8 TSP may carry out current and future risk assessments and other audits with pro-active support from the Vendor on any part of the Vendor's supply chain to identify additional risks to TSP. TSP may then stipulate additional countermeasures to address any risks. This in no means would reduce the Vendor's ultimate obligations and responsibility relating to security

4.7.9 No replacement of TSP System support tools must be undertaken by the Vendor without specific agreement from TSP.

4.7.10 If TSP agrees to the Vendor's appointment of Subcontractor under this Agreement, TSP may require that the associated security risks are clearly identified and assessed by TSP Group Security or the appropriate TSP line of business security team. This will ensure that any unacceptable security risks are identified and addressed. This in anyway shall not reduce the Vendor from being solely responsible to TSP for the ultimate obligations to be performed under this Agreement and responsibility relating to security.

4.7.11 Where TSP has approved Vendor's use of Subcontractors, formal contracts containing all necessary security requirements shall be put in place between the Vendor and its subcontractor before the Subcontractor or its personnel can access TSP Systems and TSP Information or occupy space in TSP's buildings or space in the Vendor's building that is used to access, hold or process TSP Information.

4.7.12 TSP may update from time to time, security related policies, guidelines, standards and requirements. TSP will incorporate such updates by reference which shall be notified in writing by TSP to the Vendor promptly. The Vendor is deemed to accept all the updates. If the Vendor has an issue with such updates, the Vendor shall promptly detail its concerns to TSP in writing. If TSP cannot agree on resolution of the Vendor's issues promptly, TSP reserves the right to revoke the Vendor's Authorisation and terminate this Agreement.

4.7.13 The Vendor shall record and maintain detailed information of all Contract Personnel who are authorised to Access TSP Systems or TSP Information.

4.7.14 The Vendor shall ensure that all computers or laptops used to access TSP Systems and TSP Information have their ports locked down such that removable storage media (memory sticks, removable hard drives, compact flash and secure digital cards, floppy disks, CDs, DVDs, MP3 players and other similar devices) cannot be connected.

5. Access to TSP Systems

5.1 TSP allows (so far as it can and is able to do so) the Vendor, to have Access solely for the purpose as contemplated herein during the term of this Agreement.

5.2 In relation to Access, the Vendor shall (and, where relevant, shall procure that all Contract Personnel shall):

a) ensure each individual Contract Personnel has a unique user identification and password known only to such user for his/her sole use.

b) ensure Contract Personnel never share user identification, passwords or security tokens.

c) promptly provide to TSP such reports as TSP shall from time to time require concerning the Vendor's use and security of Access and any related matters to Access.

d) ensure that physical access to fixed computer equipment having Access or storing TSP Information is solely with smart or proximity cards (or equivalent security systems) and Vendor conducts regular internal audit to ensure compliance with these provisions.

e) ensure onward bridging or linking to TSP Systems is prevented unless authorised by TSP.

f) use all reasonable endeavors to ensure no viruses or malicious code like malware, spyware, key logger, bots (as the expressions are generally understood in the computing industry) are introduced, and that there is no corruption or modification or compromisation of TSP Systems or TSP Information. This should un-doubtedly ensure that nothing results in denial of Service, interruption of Service, outages, reduction or compromise in quality and efficiency of Service, leakage or stealing of TSP Information, interference with mandated lawful interception policy, methodology & provisions, enhance risks of attacks, overbilling, frauds or any other aspect that compromises the security of all the stake holders including the Government, users, TSP etc.

g) use reasonable endeavours to ensure that personal files which contain information, data or media with no relevance to the purpose, are not stored on TSP building servers or TSP centralised storage facilities or TSP Systems.

5.3 If TSP has provided the Vendor with Access to the Internet/Intranet, the Vendor shall, and shall ensure that the Contract Personnel, access the Internet/Intranet appropriately. It is the Vendor's responsibility to ensure that practical guidance on internet and email abuse (as amended) is communicated to the Contract Personnel from time to time.

5.4 The Vendor shall ensure that all Contract Personnel, subject to the Clauses headed "Regulatory Matters" and "Confidentiality" comply with Classifying and Handling of Information.

5.5 Any security software procured by the Vendor shall be used by the Vendor without modification, unless there is an essential need to do so, in which case appropriate controls shall be applied and the agreement of TSP Group Security sought.

6 Access to Vendor Systems

6.1 If Contract Personnel is granted Access to Vendor Systems having bearing on TSP data, information or network, the Vendor shall:

a) ensure each individual has a unique user identification and password known only to such individual for his/her sole use.

b) promptly provide to TSP such reports as TSP shall from time to time require,, concerning the Vendor's use and security of access to Vendor Systems.

c) allow Access only to the minimum extent required to enable the Contract Personnel perform their duties.

d) allow Access using a secure login process.

e) establish and implement formal procedures to control the allocation and de-allocation of Access rights.

f) ensure that the allocation and use of enhanced privileges and access to sensitive tools and facilities in Vendor Systems are controlled and limited to only those users who have a business need.

g) ensure that the allocation of user passwords to Vendor Systems that hold or access TSP Information is controlled through a formal auditable management process.

h) conduct regular reviews of user ids and their Access rights.

i) provide processes to demonstrate that remote and home working activities are only permitted where Authorised by TSP and subject to appropriate security controls within the Vendor's organisation including but not limited to remote Access by users being subject to strong authentication.

j) demonstrate that users follow security best practice in the management of their passwords.

k) implement a password management system which provides a secure and effective interactive facility that ensures quality passwords.

l) ensure that user sessions are terminated after a defined period of inactivity.

m) ensure that audit logs are generated to record user activity and security-relevant events and securely managed and retained with nil ability on the part of the Vendor to allow any un-authorised access or amendment to the audit logs. Such audit logs must be maintained for future reference for a period of at least one year.

n) ensure that monitoring of audit and event logs and analysis reports for anomalous behaviour and/or attempted unauthorised access are performed by Vendor's staff independent of those users being monitored.

o) make available audit logs where required by TSP for review.

p) ensure all systems holding, processing or accessing TSP Information shall be hardened to TSP standards (Note to Buyer: If in doubt, please contact TSP Security).

q) ensure that to the extent possible, development, test and live environments are segregated from each other and the other work areas in Vendor buildings.

r) implement controls to detect and protect against malicious software and ensure that appropriate user awareness procedures are implemented.

s) ensure that Vendor has in relation to all Vendor Systems formal security incident management procedures with defined responsibilities.

t) ensure that any unauthorised software is identified and removed from Vendor Systems holding, processing or accessing TSP Information.

u) ensure that Access to diagnostic and management ports as well as diagnostic tools are securely controlled to TSP's reasonable satisfaction.

v) ensure that Access to Vendor's audit tools shall be restricted to Relevant Contract Personnel and their use is monitored.

w) Ensure that data gathered after running audit tool is properly protected.

x) perform enhanced independent code reviews (including penetration testing) on all Vendor Systems.

6.2 The Vendor shall demonstrate to TSP that Contract Personnel who hold and use the Information on PCs and mobile computing devices are responsible for ensuring that the PCs and mobile computing devices are protected from unauthorised access. Consideration must be given to whether Sensitive Information must be stored on mobile computing devices. All Sensitive Information shall be encrypted if stored on a mobile computing device or in the event of any transmission of Sensitive Information by Contract Personnel outside of TSP's trusted network. Laptops and PCs containing Sensitive Information shall have the whole of the disk encrypted. Devices that do not allow whole-disk encryption such as memory sticks, CD/DVDs, shall be subjected to additional controls such as:

(a) Use of file encryption, where available; or
(b) Use of application password facilities; and
(c) Where the device is "pocket-sized", it must be kept with the owner at all times.

Black-berry mobile phones and other such devices which use proprietary encryption technique should not be used for holding TSP information.

6.3 To the extent the servers are used to fulfill the purpose of this Agreement, Vendor's servers shall not be deployed on un-trusted networks without appropriate security controls.

6.4 Changes to individual Vendor Systems shall be controlled and subject to formal change control procedures. All documentation relating to Vendor Systems shall be protected from unauthorized Access or amendment.

6.5 Security procedures and controls shall be used to secure equipment holding, accessing or processing TSP Information in Vendor Systems.

7. Conditions for Equipment Vendors:

7.1 Conformance to Security Standards and Policies:

The vendor shall ensure and certify that the supplied equipment has been subjected to penetration testing and all addressable vulnerabilities have been mitigated and the equipment is 'Safe to Connect' in the Telecom Network as per the latest standards and recommendations on the subject from ITU/ISO/IETF/IEC etc. It will also include that the equipment confirms to the security policies of the TSP with respect to network elements. This applies to all telecom network elements and IT equipment used in the network.

The vendor shall also ensure that the equipment supplied has all the contemporary security related features, facilities, hardware, software etc for the purpose of Interception, Monitoring, Analysis etc for use by the Law Enforcement Agencies and provide complete information to enable these features and facilities before the supply of the equipment or the procedure of enabling these, if these are to be enabled after the commissioning of the Network. The Vendor shall also submit a test report on these features and facilities and also a certificate that all contemporary features and facilities of this category exist in the equipment supplied.

7.2 Submission of Test Reports:

7.2.1 General:

A report of the tests conducted with results of the tests conducted and mentioning areas where vulnerability exists and what precautions are to be taken by the TSPs to minimize the effect of such vulnerabilities. For this purpose additional requirements may be provided in the Solution Designs. Compliance statements should be made against the relevant Security Standards and where practicable, tests performed to demonstrate compliance.

7.2.2 Port Enumeration

Port and protocol scans must be conducted with reference to the network design, proving that management protocols are only accessible via management interfaces, and control plane protocols are only accessible via control plane interfaces.

All interfaces where the network element can be identified (where it would be possible to respond to a PING request or appear in a route trace) must be tested. If the interface switches/routes traffic transparently or is not IP based then that interface need not be scanned.

Scans should be performed with all Access Control Lists (ACLs) first disabled, so as to give a clearer view of which ports/services are active, and then enabled, to demonstrate what is normally visible.

Tests should detail:

- *Which addresses were scanned (management, interface).*
- *All open, open\|filtered and closed\|filtered ports*
- *Detail why ports which are open are required.*

Port scan may be performed using latest version of nmap or any other open source software tool.

7.2.3 IP Vulnerability Scanning

Service vulnerability audits must be conducted with reference to the results of the port/protocol scans and the network design.

The audit should detail:

- Low, medium and high risk vulnerabilities so that risk assessments can be made and fixes implemented where necessary
- List any mitigations to medium and high risk.

7.2.4 Compliance to AAA Design

Where a Network Element supports either RADIUS or TACACS+ for authentication, authorisation and accounting of user accounts compliance to the TSP AAA Design should be confirmed and demonstrated and test report submitted.

7.3 Equipments Configuration Guide

Two sets of equipment configuration guide should be supplied which detail the configuration required to meet the policies in the standards at least in respect of following:

Network Element security policies:

- Generic OS
- Technical Standard for Switches and Routers
- Management Standard for Switches and Routers

7.4 Additional Security Tests for Telecommunication Equipments

i) A report must be submitted in respect of following additional tests.

i. Firmware inspection

ii. Basic validation of physical device integrity at least in respect of following Core network elements

i. Main GSM Network peripherals (BSC, PCU, MSC/VLR, HLR, SGSN, GGSN)

ii. Main CDMA Network peripherals (BSC, MSC, GMSC, PCF, PDSN)

iii. Billing Systems & Servers for both GSM and CDMA network

ii) A test report on workstation Configuration & Integrity in respect of the following:

i. Administrators workstations and lab stations

ii. User workstations

7.5 A report on the susceptibility to the attacks on mobile networks:

Mobile Network like GSM equipment and its network are susceptible to several attacks. A few of the known attacks with their description are given in **Appendix II**. The vendor must submit a report categorically stating that out of these attacks or any other attack to which the equipment and the network is susceptible, the degree of risk of each type of attack and mitigation technique to deal with these attacks. The vendor will ensure that whatever mitigation was possible as per the current available technologies, techniques, configuration have already been used and adopted by them before the supply of the equipment.

Similarly, for the CDMA Network Managers it may be re-ensured that the security features such as OS hardening, user access and operation audit, privilege-based user groups, centralized authentication, user profile and group management, customer plug-ins for authentication and secure remote access with IP Security Protocol (IPSec) and other capabilities in upgrading releases as well have been provided.

Subscriber authentication to protect the infrastructure and to prevent unauthorized access to network resources:

CDMA 1X access authentication is accomplished by means of a authentication signature that is verified by the network's databases of user information. The Home Location Register and Authentication Center as well as 1xEV-DO algorithm in OTASP to exchange keys between the mobile device and the Access Node-Authentication Authorization Accounting (AN-AAA) server should be thoroughly tested by the Vendor and reported. The authentication key exchange protocols ensures the identity of the mobile device.

For CDMA2000 1X data sessions and EV-DO, including the Challenge Handshake Authentication Protocol (CHAP) or upgraded equivalent by the Packet Data Serving Node-Authentication Authorization Accounting (PDSN-AAA), server should not be compromised in any case and the tests reported.

7.6 Security from Malware:

There are no known cases of malware disrupting telecom services, yet. However, malware can cause information leaks and can result in the leak of private user information.

However, some viruses, worms and Trojans can infect devices and spread malware via text messages or Bluetooth connectivity. This network-based service will also block Denial of Service attacks and restrict network traffic based on source, destination, IP ports and applications. It will also allow enterprise IT managers to lock and/or delete data on lost or stolen devices. The connectivity could affect platforms if adequate firewalls, IDPs are not strong. Therefore vendors would provide adequate firewall and IDPs and submit a certificate in this regard.

7.7 Cryptography Related Security Issues:

Vendors will take suitable measures to deal with cryptography related vulnerabilities and submit a report of the measures along with a certificate that they have taken adequate measures to deal with these vulnerabilities**.**

i. Attacks on COMP-128 algorithm
ii. Compromised cipher key
iii. Key recovery allowing SIM cloning
iv. Hijacking outgoing calls in networks with encryption disabled
v. Hijacking outgoing calls in networks with encryption enabled
vi. Hijacking incoming calls in networks with encryption disabled
vii. Hijacking incoming calls in networks with encryption enabled
viii. Suppressing encryption between the target user and the intruder
ix. Suppressing encryption between target user and the true network

7.8 Data Flow Attacks

Many sophisticated attacks disguise themselves in data flows across sessions and ports—the more traffic there is, the harder it is to identify the threats. Vendors may ensure that they are aware of this and take adequate steps to make it future proof and submit compliance on the same.

7.9 Additional Interfaces

Many of the problems in the Data intensive infrastructure may come to increased number of interfaces additionally for Data than those were present for voice only initial 2G systems, hence, infra vendors must give special attention to interfaces and their related vulnerability. Such vendors may ensure that they provide additional notes that they have taken care of the same and the test mechanism and methodology adopted by them with adequate evidence. Some of these interfaces are listed below:

Gi: Exposed to Internet and corporate networks

Gp: Primary interconnection pt. between operator's n/w and un-trusted external networks

Gc: Allows access (via HLR) to key user info. from remote network during roaming

Vulnerable Interfaces

Gi: Exposed to all threats from Internet: viruses, DoS, and malicious network traffic

Gp: Connection hijacking, overbilling from a roaming network during handover

Gn: Not encrypted by default

7.10 Security Against Remote Access:

The vendor shall submit a written undertaking to the TSP clearly identifying all possible means of remote control/ remote access/remote command and control in the supplied equipment as well as suitable mitigation means to close such access mechanisms.

Note:

The security related test listed here in the sample template are not exhaustive and are indicative. The list is a guideline to the provider to verify that the vendor has tested against the vulnerabilities and reported the outcome of the tests in a comprehensive test report made available to him. All required security related tests as available and applicable must be performed.

7.11 Software and Hardware Design Surety;

Depending upon the robustness the service provider desires for continuity of his business TSP can include clauses on safety and security of software and hardware design; such as

7.12.1 The Vendor shall at TSP's request enter into an escrow deposit arrangement in respect of all Information and documentation in relation to Supplies in respect of Hardware, executable Software/source code/gold build etc, High Level Designs (HLD), Detail Design Documents (DDD), listings and programmer's notes) ("the Escrow Information") as would enable TSP to complete any outstanding obligations of the Vendor under this Agreement, including, without limitation, obligations that would have existed (including the requirement to fulfill any orders that TSP would have otherwise placed under this Agreement) had this Agreement not been terminated by TSP (other than pursuant to of the Condition headed "Termination") before the expiry of its natural term.

7.12.2 Without affecting any other rights it may have, TSP shall have the right, free of charge, to use the Escrow Information, after its release, in order to use or maintain (including to upgrade) the Software, to modify or have modified the Software, and to authorize such modified Software to or have it maintained by third parties, in case vendor refuse to do so as per contract agreement.

~~7.12.3~~ The Vendor shall ensure that the Escrow Information deposited in accordance with para 7.12.1 above is and will be maintained as sufficient to allow a reasonably skilled programmer or analyst to maintain, modify and correct the Hardware and Software without the help of any other person or reference, and the Vendor further undertakes to keep the Escrow Information fully up-to-date throughout the Term.

7.12.4 On the occurrence of any event permitting the release of the Escrow Information, the Vendor shall immediately provide, at its cost and expense, to TSP for a reasonable period, such advice, support assistance, data, information, access to Vendor's personnel or any key personnel of legal owner of the [Hardware and/or] Software for the purpose of understanding, maintaining (including upgrading), modifying and correcting any of the Hardware and/or Software. The softwares and codes written only in ENGLISH language shall be acceptable. The code/softwares shall be proven to be operational and correct version and to be certified that it does not have self-destructing programmes. This may be ensured by using the same at least once for loading the system initially before being deposited.

The TSP may engage the service of any escrow service agency if it opts for escrow arrangement. In such case it would be mandatory to avail the service of Indian agency, if available.

Alternative to ESCROW could be to have: -

- Gold software copy or the Executable copy of the software
- Dumb hardware can be loaded with software by the TSP or under the supervision of TSP from Gold software copy or from the executable copy after checking that hardware is free from any software and ensuring that there are no harmful malware into the hardware.
- Upgradation of software for a period of number of years (say 7 years)
- Design of network in digital form and/ or in hard copy

7.13 Penalty:

The TSP may insert suitable penalty clauses in their agreement with Vendors/suppliers. However, it must be included in the agreement that in case of inadequate measures, act of intentional omissions, deliberate vulnerability left into the equipment or in case of deliberate attempt for a security breach, the Licensor may at its discretion blacklist the vendor from making any supply deals with Indian Operators.

7.14 Inspection:

The Vendor/Supplier must 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 at the time of procurement of equipment and upto two more times every year until the supplies under the contract have been completed, at the time of discretion of the telecom service provider. All the documents should be in English and handed over to the visiting team at least 4 weeks ahead of the visit.

7.15 **Language of Supplies**:

All the software codes, firmware, operating system, hardware details should be in **ENGLISH** only.

8 Data Protection:

8.1 The Parties acknowledge that, in respect of all Personal Data and processed by the Vendor for the purpose of the provision of Supplies under this Contract, TSP alone as data controller shall determine the purposes for which and the manner in which such Personal Data will be processed by the Vendor.

8.2 Other than at TSP's request, or where required by law to provide the supplies, the Vendor shall not disclose or allow access to any Personal Data other than, subject to Paragraph 8.4(f) to a person placed by the Vendor under the same obligations as contained in this Condition who is employed or engaged by the Vendor or within the control of the Vendor in the performance of the Contract.

8.3 The Vendor shall not use Personal Data for any purpose other than the provision of the Supplies and shall return any Personal Data to TSP immediately upon request at any time providing such return does not prevent the Vendor from fulfilling its obligations under this Contract. The Vendor shall retain Personal Data no longer than is necessary for the provision of the Supplies, in accordance with the relevant Data Protection Legislation and such instructions as TSP may provide from time to time. Upon expiry or termination of this Contract for whatever reason, the Vendor shall immediately return to TSP all Personal Data and certify that no copies have been made or retained by the Vendor or any third party acting on its behalf.

8.4 The Vendor shall:

(a) process Personal Data only on the instructions of TSP and to the extent necessary for the performance of this Contract; and

(b) not modify, amend or alter the contents of the Personal Data except as required or permitted by this Contract or with TSP's prior written consent; and

(c) implement the appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, which measures are set out in more detail in Condition headed "Security of Information" and provide to TSP a written description of the measures taken when requested by TSP; and

(d) comply with all relevant provisions of any TSP codes of practice notified to the Vendor from time to time and the Data Protection Legislation; and

(e) keep all Personal Data secure and confidential, act only on TSP's instructions with respect to it, and comply with such further reasonable requirements from time to time of TSP for the security of it; and

(f) ensure that, of the Vendor's staff, only those of the Contract Personnel who need to have access to the Personal Data are granted access to the Personnel Data only for the purposes of the performance of this Contract and the Contract Personnel are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Condition; and

(g) notify TSP forthwith, and in any event, no later than 12 hours from the time it comes to the Vendor's attention, that Personal Data transferred by TSP to the Vendor has been the subject of accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any other unlawful forms of processing; and

(h) notify TSP in the event that it receives a request or notice from any data subject to have access to that person's Personal Data held by it and will provide TSP with full co-operation and assistance in relation to any complaint or request including providing TSP with any relevant Personal Data it holds within the timescales provided by the request or notice or as otherwise required by TSP.

8.5 In respect of Transfer of Personal Data the following conditions shall apply:

(a) obtain TSP's prior written consent before transferring Personal Data to any Subcontractors in connection with the provision of the Supplies;

(b) prior to any Transfer of Personal Data, enter into or procure that any Subcontractor delivering the Supplies will enter into contracts for the transfer of personal data. In respect of Personal Data transferred by TSP to the Vendor or acquired by the Vendor from TSP's systems to a country outside of India shall be on the basis of the Legislation issued by the Indian Government, or such other data protection model contract terms as may be agreed between the Parties from time to time, except where the relevant Data Protection Legislation provides for a derogation from this requirement.

8.6 Any breach of this Condition by the Vendor shall be deemed to be a material breach of the Contract and the Vendor shall indemnify TSP from the against any costs, losses, damages, proceedings, claims, expenses or demands incurred or suffered by TSP which arise as a result of such breach.

8.7 The Vendor shall, upon TSP giving reasonable notice, allow TSP or its nominated representatives such access to its premises, Information and records and those of its agents subsidiaries and sub contractors, as may be reasonably required by TSP from time to time to assess the Vendor's and/or Contract Personnel's compliance with this Condition.

9 Regulatory Matters

9.1 The Vendor shall

(a) comply with all Regulatory Matters including, without limitation, any actions that TSP may require in connection with any Regulatory Matter, that are notified to the Vendor Regulatory Contact from time to time by the TSP Regulatory Contact in so far as they relate to the performance of the Contract by the Vendor;

(b) within 14 days of the Commencement Date, ensure that the Vendor Regulatory Contact contacts the TSP Regulatory Contact to establish the nature and extent of communication between them, which assist them in meeting all regulatory requirement as set by licensor or Sectoral regulator or any other person nominated by Licensor.

(c) ensure that the vendor and its Contract Personnel have undergone the proper and adequate Training for the purpose of execution of this agreement;

(d) promptly provide such information to TSP as shall be necessary for TSP to respond fully and to the timescale required to any request or requirement for information from a government or any regulatory authority, to the extent that such information relates to the performance of the Agreement by the Vendor; and

(e) permit TSP and/or its authorised agents such access to the Vendor's premises and such Access to and copies of its Information and Records (and to and of those of any Contract Personnel) as is required by TSP to assess and/or validate the Vendor's performance of its obligations under or in relation to this Clause.

10 Confidentiality

10.1 In this Clause, TSP Information which TSP from time to time identifies to the Vendor as being commercially confidential, or is by its nature commercially confidential or defined by TSP as confidential, or confidential as per the applicable law.

10.2 Except with TSP's agreement, the Vendor shall not disclose Information to any TSP employee, not authorized to receive

10.3 Subject to the Condition headed ‘Intellectual Property”, either party receiving Information ("the Recipient") from the other shall not without the other’s prior written consent use such Information except for Contract purposes or disclose such Information to any person other than TSP's employees, agents and contractors or Contract Personnel who have a need to know and who are bound by equivalent obligations of confidentiality. Any breach of such obligations by Contract Personnel or TSP's employees, agents or contractors (as the case may be) shall be deemed to be a breach by the Vendor or TSP respectively.

10.4 Paragraphs 2 and 3 of this clause shall not apply to Information that is:

(a) published except by a breach of the Contract; or

(b) lawfully known to the Recipient at the time of disclosure and is not subject to any obligations of confidentiality; or

(c) lawfully disclosed to the Recipient by a Vendor without any obligations of confidentiality; or

(d) replicated by development independently carried out by or for the Recipient by an employee or other person without access to or knowledge of the Information.

10.5 The Vendor shall not publicise this Agreement without TSP's prior written consent and shall ensure that any subcontractor is bound by similar confidentiality terms to those in this clause.

10.6 Either party that has during the course of this Agreement received Information in a recorded form from the other (or has recorded received Information) shall return or destroy in a complete irrecoverable mode (at the option of the disclosing party) such records upon:

(a) expiry or termination of this Agreement; or

(b) upon earlier request

unless such records are part of the Supplies.

10.7 This clause shall survive termination / expiry of this Agreement.

11. Intellectual Property

Each Party will retain its right, title and interest in its respective trademarks, service marks and trade names as well as rights in respect of any patent, copyright, trade secrets or other intellectual property used during the performance of this Agreement. Both Parties recognise that except as otherwise expressly provided herein or agreed between the Parties, they shall have no right, title, interest or claim over the others' intellectual property.

12. Security Review

The Vendor shall:

(a) give to (or procure the giving to) TSP (or any person authorised by TSP) such access at all reasonable times to the Vendor's and any Subcontractor's records and premises related to this Agreement as TSP may require from time to time to assess the Vendor's compliance of these policies in this Agreement; and

(b) such assessments may include assessments of all elements of physical and logical audits, penetration testing of the Vendor's Systems. The Vendor shall facilitate this assessment by permitting TSP to collect, retain and analyse information to identify

potential security risks including trace files, statistics, network addresses and the actual information or screens accessed or transferred; and

(c) provide such reports to TSP and attend such meetings as may be reasonably required by TSP.

13. **Network Audit, Test And Certification**:

The process of networks Audit and certification should be performed by Third Party/Parties to include following activities:

(I) **Network forensics** to identify existing unwanted running processes\ malwares\ backdoors etc. on all networks' elements. The operation includes sniffing of live traffic to identify unwanted redirection and interception of traffic.
(II) **Network Hardening** to map all networks elements and to calibrate them to optimized secured state.
(III) **Network penetration test** to assure system durability against any kind of attack.
(IV) **Risk assessment** to understand what actions should be taken to minimize future damage to carrier and what risks are inevitable.
(V) **Actions** to fix found problems by setting systems to default or acquiring relevant IT security technologies to prevent such problems from reoccurring.

An available list of Test and Certification Agencies (Third Parties) in various countries who may take up the regular Technical Audit of Networks and Security Certification is given at Appendix I. The TSP may engage the services of any other Network Audit and Security Certification agency also.

14 Investigation:

14.1 If TSP believes that there has been a breach by the Vendor of the provisions of this Agreement, TSP will inform the Vendor Security Contact. The Vendor shall cooperate with TSP fully in any ensuing investigation. The Vendor shall provide list of users who have had access to TSP Systems and TSP Information to TSP and/or any law enforcement agency. TSP shall have access to the Vendor Systems and TSP Information in the Vendor's premises generally with prior notice but include the right to make unannounced visits.

14.2 The Vendor shall report to TSP Security Contact promptly of any potential misuse of TSP Information or improper or unauthorised access to TSP Systems and TSP Information. Upon request, the Vendor shall promptly provide to TSP a written report with details of the potential misuse of TSP Information or improper or unauthorised access to TSP Systems and TSP Information, a remedial plan and a timetable for achievement of the planned improvements and steps to be taken to avoid the repeat of the potential misuse of TSP Information or improper

or unauthorised access to TSP Systems and TSP Information. Please see note at the end of the clause 14.

14.3 If any audit or investigation reveals that there is a potential risk to the confidentiality, integrity or availability of TSP Information in the Vendor's processes or Vendor Systems, Vendor shall promptly correct any security risk in the Vendor's processes or Vendor Systems promptly.

14.4 During investigation, the Vendor shall co-operate with TSP, providing reasonable access, accommodation, facilities and assistance to all Vendor Systems as reasonably necessary to investigate the breach of the provisions of this Agreement including permitting interview of any sales, engineering or other operational personnel of Vendor. TSP shall, or at TSP's request shall instruct the Vendor to, confiscate for evaluation any tangible or intangible asset suspected to have been used for information/ security breach or provide lead to investigation belonging to the Vendor or its subcontractor to aid the investigation.

Note: The clause No. 14.1 to 14.4 relates to investigation of all the security aspects and other relevant provisions contained in the earlier paras/clauses.

15 ***Limitation of Liability:*** *TSP may have appropriate clause on the issue.*

16 Termination

This Agreement shall be effective from the date hereof and shall continue to be in full force and effect concurrently with the Vendor agreement ("**Term**") unless terminated earlier by TSP in accordance with the provisions below.

In the clause specifying the conditions of termination of contract, it should also be mentioned that '***The Contract may also be terminated on directions of the Licensor alongwith Penalty under the Laws of the land in India in relation to security breaches noticed'***.

Without prejudice to TSP's rights and remedies under the Agreement, the Vendor shall at its own cost and expense take all steps necessary to restore the lost or corrupted TSP Information to the last back-up and/or terminate the unauthorised use of or access to the Information to the extent it caused such loss, corruption or unauthorised use of the TSP Information, due to act of omission or commission on the part of vendor.

Termination Clause may be inserted by TSP keeping in view the type of contract agreement w.r.t. service availed.

17 Law and jurisdiction

This Agreement is governed by Indian law and subject to clause 18, Parties agree to the exclusive jurisdiction of the Indian courts where the registered office of the TSP is situated.

18 Arbitration

Any dispute arising out of this Agreement shall be settled and resolved as per the dispute resolution and arbitrations clause agreed between the Parties under the Supply & Services Agreement.

19 Notices

All notices, requests, consents, waivers or other communication required or permitted hereunder shall be delivered as per the Notice clause agreed between the Parties under the Supply & Services Agreement.

Appendix I

List of Test and Certification Agencies (Third Parties) in various countries who may take up the regular Technical Audit of Networks and Security Certification.

The List is indicative and Licensee may use the services of other Network Audit and Security Certification agency also.

CC Evaluation Labs

Australia and New Zealand

1 Computer Sciences Corporation (CSC)

http://www.csc.com/security/offerings/26694-common_criteria_at_csc

Contact: Andrew Coggle
212 Northbourne Avenue
Braddon ACT 2612
Tel: +61 2 6246 8000
Fax: +61 2 6246 8181
E-mail: aisef@csc.com.au
Web: http://www.csc.com/commoncriteria

2 Logica

http://www.logica.com.au/

Contact: Bruce Legge
1 Torrens Street
BRADDON ACT 2612
Tel: +61 2 6246 1900
Fax: +61 2 6262 8827
E-mail: aisef.au@logica.com
Web: http://www.logica.com/au

3 Startsec

http://www.stratsec.net/Home

Contact: Aleks Lubiejewski
Unit 1, 50 Geils Court
DEAKIN ACT 2600
Tel: +61 2 6260 8878
Fax: +61 2 6260 8828
E-mail: lab@stratsec.net
Web: http://www.stratsec.net

Germany

1 CSC Deutschland Solutions GmbH

Contact: Herrn Dr. Goswin Eisen
Sandstr. 7-9
80335 München
Telefon: +49 89.5908.6504
Fax.: +49 89.5908.6503
E-Mail: geisen@csc.com
Web: http://www.csc.com/security/ds/11371/15880-german_laboratory_experience

2 atsec information security GmbH

http://www.atsec.com/us/addresses-contact.html

Contact: Gerald Krummeck
Steinstr. 70
81667 München
Telefon: 089 44249-830
Fax: 089 44249-831
E-Mail: gerald@atsec.com
Web: http://www.atsec.com

United Kingdom

1 EDS

http://h10134.www1.hp.com/

2 Logica

www.logica.com

3 SiVenture

http://www.siventure.com

USA

1 Arca Common Criteria Testing Laboratory

http://www.savvis.net/en-US/Pages/Home.aspx

Contact: Pete Feeney
45901 Nokes Boulevard
Sterling, VA 20166
Tel: +1 703-667-6684
Fax: +1 509-691-7440
Mobile: +1 703-999-1075
E-mail: arca-cctl@savvis.net

2 CygnaCom Solutions' Security Evaluation Laboratory

http://www.cygnacom.com/labs/common-criteria/index.htm

Contact: Ms. Nithya Rachamadugu
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102-3305
Tel: +1 703.270-3563
Tel: +1 858-509-0180
Fax: +1 703-848-0985
E-mail: selinfo@cygnacom.com
Web: http://www.cygnacom.com

3 SAIC Common Criteria Testing Laboratory

http://www.saic.com/infosec/testing-accreditation/common-criteria.html

Contact: Robert L. Williamson
Ctr. for Information Security Tech. SAIC
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046
Tel: +1 410-953-6819
Fax: +1 410-953-7001

E-mail: robert.l.williamson.jr@saic.com
Web: http://www.saic.com

4 Computer Sciences Corporation (CSC)

http://www.csc.com/security/offerings/26694-common_criteria_at_csc

Contact: Charles Nightingale
7231 Parkway Drive
Hanover, Maryland 21076
Tel: 443.445.8400
Fax: 443.445.8002
E-mail: STCL@csc.com
Web: http://www.csc.com/commoncriteria

5 *Booz Allen Hamilton Common Criteria Testing Laboratory*

900 Elkridge Landing Road, Suite 100, Linthicum, MD 21090

http://www.boozallen.com/doingbusiness/contractvehicles/gmacs/alliant/alliant/38447966/38470558

6 *COACT Inc. CAFE Laboratory*

9140 Guilford Road
Suite N, Columbia, MD 21046-2585

http://www.coact.com/

7 DSD Information Assurance Laboratories (DIAL)

1160 Johnson Ave.
Suite 101, Bridgeport, WV 26330

http://dsdial.com/

8 InfoGard Laboratories, Inc.

709 Fiero Lane
Suite 25, San Luis Obispo, CA 93401

http://www.infogard.com/

Taiwan (not from CC portal)

Telecom Technology Center, Taipei, Taiwan

http://www.ttc.org.tw/english/its_e.asp

http://www.ttc.org.tw/english/its_e_01.asp

The Nederlands

Brightsight IT Security Evaluation Facility

Contact: Mr. Dirk-Jan Out
Delftechpark 1
2628 XJ Delft
The Netherlands
Telefon: +31 15 269 25 00
Fax: +31 15 269 25 55
E-Mail: info@brightsight.com
Web: http://www.brightsight.com

Israel

ALTAL Security Consulting, Israel

http://www.altalsec.com/index.php?langpage=eng&&language=eng

Canada

Electronic Warfare Associates (EWA), Canada

http://www.ewa-canada.com/

Routers Tested as per CC:

Cisco Routers

Cisco Systems Routers (800, 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200 running Cisco IOS Release 12.4(11)T2; 7300, 7400, and 7600 running Cisco IOS Release 12.2(18) SXF8; 10000 and 12000 running 12.0(32)s7) and Cisco Secure ACS version 4.1.2.12

TOE evaluation was sponsored by Cisco Systems, San Jose

Evaluation was carried out by: "*Arca Common Criteria Testing Laboratory"*

http://www.savvis.net/en-US/Pages/Home.aspx

Contact: Pete Feeney
45901 Nokes Boulevard
Sterling, VA 20166
Tel: +1 703-667-6684
Fax: +1 509-691-7440
Mobile: +1 703-999-1075
E-mail: arca-cctl@savvis.net

Juniper Routers

Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14

ST was prepared by:

Science Applications International Corporation(SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

http://www.saic.com/

Evaluation was carried out by:

Science Applications International Corporation(SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

http://www.saic.com/

VoIP equipments tested as per CC:

AVAYA VoIP PBX System

ST prepared by:

CSC Deutschland Solutions GmbH

Contact: Herrn Dr. Goswin Eisen
Sandstr. 7-9
80335 München
Telefon: +49 89.5908.6504
Fax.: +49 89.5908.6503

E-Mail: geisen@csc.com
Web: http://www.csc.com/security/ds/11371/15880-german_laboratory_experience

Evaluated by:

CSC Deutschland Solutions GmbH

Contact: Herrn Dr. Goswin Eisen
Sandstr. 7-9
80335 München
Telefon: +49 89.5908.6504
Fax.: +49 89.5908.6503
E-Mail: geisen@csc.com
Web: http://www.csc.com/security/ds/11371/15880-german_laboratory_experience

Appendix II

Some of the known types of attacks on GSM and CDMA networks

- Eavesdropping

  This is the capability that the intruder eavesdrops signalling and data connections associated with other users. The required equipment is a modified MS.

- User Impersonation

  An intruder sends signalling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The required equipment is again a modified MS.

  - De-registration spoofing

    An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. The intruder spoofs a de-registration request (IMSI detach) to the network.The network de-registers the user from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for mobile terminated services.

  - Location update spoofing

    An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface.The user spoofs a location update request in a different location area from the one in which the user is roaming.The network registers in the new location area and the target user will be paged in that new area.The user is subsequently unreachable for mobile terminated services.

  - Passive Identity Caching

    A passive attack that requires a modified MS and exploits the weakness that the network may sometimes request the user to send its identity in cleartext.

  - Active Identity Caching

    An active attack that requires a modified BTS and exploits the weakness that the network may request the MS to send its permanent user identity in cleartext.An intruder entices the target user to camp on its false BTS and subsequently requests the target user to send its permanent user identity in cleartext perhaps by forcing a new registration or by claiming a temporary identity mismatch due to database failure.

- Impersonation of the network

This is the capability whereby the intruder sends signaling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. The required equipment is modified BTS.

- Camping on a false BTS

  An attack that requires a modified BTS and exploits the weakness that a user can be enticed to camp on a false base station.Once the target user camps on the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered.

- Camping on false BTS/MS

  An attack that requires a modified BTS/MS and exploits the weakness that a user can be enticed to camp on a false base station.A false BTS/MS can act as a repeater for some time and can relay some requests in between the network and the target user, but subsequently modify or ignore certain service requests and/or paging messages related to the target user.

- Man-in-the-middle

  The intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signaling and user data messages exchanged between the two parties. The required equipment is modified BTS in conjunction with a modified MS.

- Compromising authentication vectors in the network

  The intruder possesses a compromised authentication vector, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signalling messages on network links.

- Overbilling Attack

Involving a malicious user hijacking a subscriber's IP address and then using that connection to initiate fee-based downloads or simply use that connection for their own purposes. In either case, the legitimate user is billed for activity which they did not authorize or actually conduct.

- Spoofed PDP context

Exploiting the weakness in the GTP (GPRS Tunneling Protocol)

- Spoofed delete PDP context packets

Which would cause service loss or interruption for end users

- Spoofed create PDP context packets

Which would result in unauthorized or illegal access to the Internet or customer data networks

- GTP packet floods

Which is a type of Denial of Service attack.

- Vulnerabilities with SIP-based VoIP systems

That might allow hackers to:

Reconfigure VoIP settings and gain access to individual users' account information

Eavesdrop on VoIP communications

Hijack a user's VoIP subscription and subsequent communications.