Annexure-II

Department of Information Technology

Subject: Security of IT infrastructure deployed at Ultra Small Bank Branches.

Background

There is a proposal for providing financial services to the un-banked segment of the Indian population. The said proposal envisages to operate small branches and ultra small branches at block and village levels respectively. The proposal also envisages use of Laptop and Tablet devices which connect to the Bank's network over Virtual Private Network (VPN) so as to reduce cost overheads and utilize minimum space for banking operation and also secure the transactions between the ultra small branches and the respective banks.

The concept and the proposal is certainly feasible. It requires the appropriate security mechanism to be implemented at the Laptop/Tablet level as well as to protect the information which flows over communication links from ultra small branch to bank level branch. The Laptop available should deploy adequate security features for protection of information not only within the system but also when the information is in transit. The firewalls at software level, authentication mechanism and antivirus software may be deployed at the ultra branch level on the laptops whereas the same cannot be said with regard to Tablets. The technology with respect to Tablet needs maturity with security features. Most of the Tablets operate on Android operating system for deployment of application. Some Tablets are available in the market with the Windows operating system. However, the operating system on such Tablet does not have features to adequately protect the information within the Tablet as well as during the communication from Tablet to the banks server. In view of this, at this stage, the Tablets are not recommended to be deployed. It may also be mentioned here that the difference between the cost of Tablet and Laptop is not much. The additional cost of Laptop system provide more features both in terms of deploying applications as well as securing the processing and storage of information.

The following security guidelines are suggested for implementation on Laptop systems at the Ultra small branch:

- Only Laptops with built-in optical drive as well as hard disk drive to be deployed.
- The laptops should mandatorily deploy systems which offer secure Logon, File Level Security and the ability to encrypt data. Windows 7 operating system offer such security features and therefore the laptops should mandatorily deploy atleast Windows 7 operating system on higher versions. Versions of Windows 95, 98, XP and Vista do not offer such security features and are not recommended for use.
- The Windows 7 operating system should be patched up, updated and hardened to protect against attacks/hacking from outside.
- Open source operating system should not be used as such operating systems may not be regularly updated and patched up. Such open source operating systems require third party products for providing adequate security features which at times are vulnerable.

- Laptops should mandatorily have the commercially available antivirus systems which should be updated regularly online.
- No freely available antivirus software may be used.
- A strong BIOS password should be enabled for protecting the laptop access.
- Also ensure that the BIOS password locks the hard drive in the Laptop so that it cannot be removed and reinstalled.
- BIOS password should only be allocated by the bank and also banks should retain a copy of the same for recovery of information and password as and when necessary.
- The software firewalls deployed in the laptops should be configured with respect to the application and tested. This is because the firewall should not block any form which may be written in Java or any such language required for banking transaction.
- (The laptop must run only applications which are authorized. Laptops should not be used for general Internet browsing and any other purpose which is not connected with the operations of Ultra Small Branch).

Protection Measures

- Disable the guest Account from the Laptop
- Default Administrator Account should be disabled
- Prevent the last logged-in user name from being displayed
- Disable Infrared, Blue tooth and USB ports on the Laptop

Data Transaction over VPN

- The connectivity between the laptop at Ultra small branch and bank's networks should be established through GPRS/2000 1X.
- The connectivity between the laptop at Ultra small branch and banks network should automatically get disconnected if it remains idle for more than 15 minutes.
- Only one VPN session be allowed between the Ultra small branch and bank's network. This should be ensured by the network administrator of the bank.

Access Log Maintenance

- (The laptop must run only applications which are authorized. Laptops should not be used for general Internet browsing and any other purpose which is not connected with the operations of Ultra Small Branch).
- A backup may be taken for all the data kept in the storage of the laptop and be maintained in safe custody regularly. The bank must maintain logs of all accesses and transactions made from Laptops installed at Ultra Small Branch.
- Provisions should be made for generating alarms for transactions above certain limit at the bank end.

*****