APPENDIX (A)

Requirement for application and intermediate application In designing and implementing the National Subscriber Registry system and in addition of all requirements in the RFP, Appendices A,B and as a minimum, the system should also support the following requirements:
(These are minimum requirements and are by no means totally inclusive.)

A. Authentication:

1 All Password rules must be parameterized.

2 Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

3 Store password files separately from application system data with encryption. “if authentication is done by using different way, please inform us”

4 Store and transmit passwords in protected (e.g., encrypted or hashed) form.

B. Audit Trail & Logging:

Event Logging

1 All security relevant events must be logged on, login failures, data modification, use of privileged accounts, change to access modules or file permissions, change to users permissions, use of any privileged system functions, and all security administrator activities.

2 Log Audit should include the following:
- User IDs;
- Dates, times, and details of key events, e.g. log-on and log-off;
- Terminal identity or location if possible;
- Records of successful and rejected system access attempts;
- Records of successful and rejected data and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and the kind of access;
- Network addresses and protocols;
- Alarms raised by the access control system;
- Information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);
- Which account and which administrator or operator was involved;
- Which processes were involved?
- Activation and de-activation of protection systems, such as anti-virus systems
- Intrusion detection systems

3 Event log must be in relational database format. And the Logs output should be readable and not need to be read by vendor only:

C. Input / Output Data Validation

Input Data Validation

1 The user should not have the authority to run commands from the application even if he/she used third party tool

2 Data input to applications should be validated to ensure that this data is correct and appropriate.

3 The application should have a mechanism to checks the input of business transactions, standing data (e.g. MISDSN, names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates).

4 Dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
   a. Out-of-range values;
   b. Invalid characters in data fields;
   c. Missing or incomplete data;
   d. Exceeding upper and lower data volume limits;
   e. Unauthorized or inconsistent control data.

Control of internal processing:

1 The application should have ability to prevent man-in-the-middle and replay attacks

2 The system should have the ability to prevent programs running in the wrong order or running after failure of prior processing;

3 The System should use of appropriate procedure to recover from failures to ensure the correct processing of data;

4 The system should have a protection mechanism against attacks using buffer overruns/overflows.

Output data validation

The system must have the ability to check the Output data validation as following:

1 Plausibility checks to test whether the output data is reasonable;

2 Reconciliation control counts to ensure processing of all data;

3 Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;

4 Procedures for responding to output validation tests;

5 Creating a log of activities in the data output validation process

E. Encryption

1 If any, Encrypted must be available when transferring all transactions from TCSI & CBSI's to application server.

2 Passwords must be encrypted and in cipher text in the application servers and when transferring passwords, passwords must not be known by any staff even the administrator and must be encrypted in the database.

F. API

Support the following API's connection features:

1 The API's used should be separated and dedicated to the solution
2 The API's capacity should have exceeded the total traffic came from all mobiles.
3 The API's should have a mechanism to prevent the traffic came from untrusted source
4 The API's should have log enabled to trace any case.
5 The API's should have mechanism to detect any man in the middle attack.
6 The API should have mechanism to limit the number of open connections to operators backend.

F. Hardware / Software

1 Provide BOQ (list of hardware) to cover the solution
2 Provide list of software (list of licenses needed), and the open-source products as well.