Independent Communications Authority of South Africa
350 Witch-Hazel Avenue, Eco Point
Office Park Eco Park, Centurion.
Private Bag X10, Highveld Park 0169

ANNEXURE D – SUBSCRIBER EQUIPMENT (INCL. MOBILE DEVICE) COMPLIANCE

1. Purpose of ANNEXURE D

The purpose of Annexure D is to highlight the technical and functional requirements and specifications of the subscriber equipment compliance module which the Independent Communications Authority of South Africa (hereinafter referred to as "the Authority") is seeking to acquire. This system should identify the subscriber equipment (including in particular mobile devices) in use in the South African telecommunications market and detect the IMEIs attached to various networks in order to identify which subscriber equipment / devices are compliant with prescribed local and international standards. The module will be provided to the Authority as per the terms and conditions as set out herein.

In terms of the provisions of Chapter 6 of the Electronic Communications Act, 2005 no person may *inter alia* possess, sell or use any type of electronic communications equipment used or to be used in connection with the provision of electronic communications, unless such equipment has been approved by the Authority. To this end, the Authority has promulgated Regulations for the Type Approval of Electronic Communications Equipment and Electronic Communications Facilities and the Certification of Type Approved Equipment, 2013 (the Regulations). In terms of the Regulations, the Authority may conduct market surveillance on all equipment that requires type approval in order to ensure compliance.

2. Functional Specifications

2.1. ICASA intends to appoint a service provider to supply the subscriber

equipment compliance (Mobile Device Compliance) system.

2.1.1. The module will be used to detect all IMEIs attached to the various networks in order to identify which equipment and or devices are compliant with prescribed local and international standards.

2.1.2. The System should connect to all the Mobile Network Operators in South Africa, should receive IMEI-Check and LE-Identity-Check requests to detect all IMEIs connecting to the Mobile Operator, and shall replicate in real-time the IMEIs from all Mobile Operators in one Centralized Database located on the premises of the Independent Communications Authority of South Africa (ICASA).

2.1.3. By analyzing the centralized data replicated into ICASA's system, which is to include all handsets in the market, the System should be able to identify genuine, fake and cloned devices, and generate a comprehensive electronic communications equipment and or device repository, thereby ensuring proper identification and certification of mobile phones / devices connected to the network for compliance purposes thus ensuring consumer protection against defective / grey products. In addition, the system would be helpful to licensees in their efforts to target the right subscribers in marketing campaigns, propose the optimal device bundles, assess network investment decisions, and understand the device market.

2.1.4. The System shall support the Authority in fulfillment of its mandate to:

2.1.4.1. ensure devices are compliant with prescribed standards.

2.1.4.2. detect non-compliant devices and restrict their access to the South African network, as per a set of rules and procedures defined by applicable prescripts

2.1.4.3. detect duplicate devices in real-time that are using IMEIs of conformed devices and restrict their access to the network.

2.1.4.4. identify IMEI swapped devices (i.e. devices using an IMEI that is related to another device) and restrict their access to the network.

2.1.4.5. support the efforts by the South African Revenue Services to collect the duties attendant upon electronic communications devices by rooting out grey devices.

2.1.4.6. support law enforcement agencies with capability for verification of customer data collected by licensees for purposes of enforcement and monitoring licensees' compliance with the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.

Bidders must submit proof (e.g. datasheets, product manuals, catalogues, etc.) to confirm/verify that the proposed system conforms to the Architecture, Requirements, Technical Parameters, Special Reporting Requirements listed below:

ITEM NUMBER	BRIEF DESCRIPTION
2.1.5.	**Electronic Communications Equipment / Mobile Device Compliance ("ECE"/"MDC") System – Minimum Requirements**
	2.1.5.1. MDC System shall have the capacity to maintain the database of IMEIs of all the devices registered on the mobile networks, considering the Number of mobile subscribers in the country to be 150 million subscribers, and the total number of active IMEIs to be 200 million; 2.1.5.2. MDC System shall be able to identify IMEIs which are not allocated by the GSMA i.e. invalid IMEI, null, duplicated or otherwise unauthorized; 2.1.5.3. Database of MDC System shall contain the following information - as a minimum – for the devices detected in all the mobile networks in the Country; 2.1.5.3.1. IMEIs 2.1.5.3.2. IMEI status (white, black and grey) 2.1.5.3.3. Date of record creation 2.1.5.3.4. Date of last record update 2.1.5.3.5. Device model number 2.1.5.3.6. IMEI status reason (invalid, stolen, cloned, valid) 2.1.5.3.7. All device information in accordance with the information available in the GSMA database 2.1.5.4. MDC shall provide a Centralized Database containing all the IMEIs detected in the Mobile Network Operators, which needs to run smoothly and automatically with real-time synchronization with the local database of IMEI codes, installed in the Mobile Network Operator; 2.1.5.5. MDC must be integrated with the Operator network to collect/conduct checkIMEI and LE-Identity-Check requests, and must save the device information in the Local Database of the

	MNO, with real-time replication of this information into the centralized database of ICASA; 2.1.5.6. The system shall identify automatically the GSMA compliant devices, and allow them to function normally and freely on operators' networks; 2.1.5.7. The system shall fight against counterfeit mobile devices with fake IMEI numbers and deny their access to mobile network operators. However, the system shall keep the existing fake IMEIs operational on the network while locking the IMEI and IMSI of the subscriber with possibility of switching the locking to another IMSI by mobile operators; 2.1.5.8. The system shall detect in real time the cloned mobile devices operating on the operators' networks and deny their access to mobile network operators. However, the system shall keep the existing cloned IMEIs operational on the network while locking the IMEI – IMSI of these devices for some cases, with possibility of switching the locking to another IMSI by mobile operators; 2.1.5.9. The system shall automatically block stolen or lost mobile devices through IMEI codes across all operators. 2.1.5.10. The system shall prevent the degradation of Quality of Service, due to the network interference and congestion caused by fake and cloned devices; 2.1.5.11. The system shall provide information and real-time reports about GSMA approved, fake, cloned, locked, and unlocked mobile devices of Mobile Operators subscribers; 2.1.5.12. The system shall support white, black and at least 5 different types of gray lists of IMEI codes in response to the Check_IMEI or ME-Identity-Check requests; 2.1.5.13. The system shall support adding, removal, and updates to the central database through a series of APIs; 2.1.5.14. The System shall detect and block SIM Boxes in all the Operators; 2.1.5.15. In the event of any failure, MDC shall not disrupt in any manner the KPIs and the

	performance of the operator and shall not affect any node in the Operator. 2.1.5.16. The system shall implement an advanced audit system that will log any action performed on the servers and on the IMEI DB, and the system shall send such logs as alerts for any suspicious action;
2.1.6.	**Definitions and Abbreviations**
	SW - software; **IMEI** - international mobile equipment identity; **IMSI** - International Mobile Subscriber Identity **API** - application programming interface **REST/RESTful** (Representational State Transfer) - protocol for exchanging structured messages in distributed computing environments; **XML** - extensible markup language; **OSA** – operational-search activities; **MDC** – Mobile Device Compliance; **Record** - information on the subscriber's device, containing information in accordance with the service rules; **GSM** - Global System for Mobile Communications
2.1.7.	**Supplier Requirements**
	2.1.7.1. ~~Potential~~ supplier in the tender must provide a detailed description of the interface for interaction with mobile operators, as well as software functions. 2.1.7.2. The ~~potential~~ supplier must provide technical documentation specifying the required format of data as well as methods to generate the data; 2.1.7.3. Supplier must provide access to a demo version, to check and assess the functionalities of the system; 2.1.7.4. The supplier must be a GSMA Associate Member and shall have a valid contract with GSM association; 2.1.7.5. The supplier must provide the full platform from A to Z related to the SW and shall not rely on any third-party software. The full platform includes the EIR, Local DBs and Central DB, real-time replication between local and Central DBs, Auditing systems, cloned devices detection, fake devices detection, and any other software required for the solution; 2.1.7.6. The supplier must provide the project and process support with local and remote access to the system;

	2.1.7.7. The supplier must provide system integration requirements in the form of support by telephone for the first year on a 24/7/365 basis. 2.1.7.8. The supplier must provide the appropriate training of engineers and integrators for the installation and commissioning, as well as before/after support; 2.1.7.9. The supplier, according to the SLA requirement of 99.99%, creates a project confirmation reservation structure based on the N-way method of implementing redundancy on local sites; 2.1.7.10. The Central IMEI DB must be scalable in terms of performance by adding additional computing resources without changing the software; 2.1.7.11. The scalability of the Central IMEI DB must not have ANY impact on the configuration of other network nodes of the mobile operator; 2.1.7.12. The supplier must ensure instant communication with the GSM Association, in order to keep the IMEI DB updated with all the newly issued models in the market; 2.1.7.13. The supplier must provide an SNMP monitoring system that will alert the client to any potential problem; 2.1.7.14. If needed the supplier shall provide full support in drafting the legal documents for the project, and shall make sure that any decree required for the implementation of the Mobile Device Compliance Module covers all the aspects and rules of the project; 2.1.7.15. The supplier undertakes to schedule a visit to one country of operation where the system is currently deployed and in live mode, so that ICASA can experience the system in live mode and assess its functionalities and mechanisms. The supplier shall schedule meetings with the Ministry of Telecommunication and Mobile Network Operators, during the visit, if requested by ICASA.
2.1.8.	**Technical requirements for SW and DB – General Requirements**

	2.1.8.1. The database architecture should be reliable and able to support up to two billion combinations; 2.1.8.2. The supplied SW must support the ability to register two billion IMEI & IMSI accounts; 2.1.8.3. The supplied SW must be able to be expanded by installing additional modules without changes that would entail additional costs for the Customer or network carrier; 2.1.8.4. The supplied SW solution should provide load balancing between servers and their number; 2.1.8.5. The user interface of MDC must be executed in English language, and any other language requested by the Client; 2.1.8.6. The supplied SW must be able to be easily integrated with operators' existing Automatic Device Configuration (ADC) and Automatic Device Management (ADM) systems of the Operators. 2.1.8.7. Automatic and real-time synchronization of local databases of mobile operators with the data of the Central IMEI Database; 2.1.8.8. Automatic and real-time synchronization of the Central IMEI Database with the local databases of mobile operators; 2.1.8.9. Automatic synchronization of the central IMEI database with the GSM Association database 2.1.8.10. Collection and processing of real-time statistical data about all IMEI codes; 2.1.8.11. Storage of all versions of the IMEI codes for at least 4 years; 2.1.8.12. Support 14-, 15-, and 16-digit formats of IMEI code 2.1.8.13. Provide access to local and central systems based on multiple user access roles such as read-only, read and write, admin, support agent, operation agent, etc. 2.1.8.14. Availability of a test environment for verifying the health of all participants in the process 2.1.8.15. Automation of testing procedures after making changes to the SW settings. Step-by-step testing and changes mode, listing possible errors and registration in the completed tasks log, must be available; 2.1.8.16. The central MDC SW should process at least 4000 requests per second;

	2.1.8.17. SW update without stopping the provision of services; 2.1.8.18. The solution must have modular capabilities to store databases. It is therefore important that the supplier can integrate its system with any of the databases through a standard interface. 2.1.8.19. The software must be compatible with 2G/3G/4G and 5G networks 2.1.8.20. Replacement and maintenance of equipment without termination of MDC-related services; 2.1.8.21. Restoring the previous version of the SW without termination of MDC-related services, in case of failures in the new version of the SW; 2.1.8.22. Support for SW backup mechanisms as well as configuration and data on internal and external media; 2.1.8.23. Storage of information on internal / external media; 2.1.8.24. Support recovery after backup failure in automatic and manual modes; 2.1.8.25. Support for Disaster Recovery (DR) site 2.1.8.26. Synchronization with the exact time source using the C-NTP Protocol 2.1.8.27. In the IMEI database it should be possible to apply procedures and restrictions for one or more SIM cards (application of the IMSI range policy) or IMEI numbers; 2.1.8.28. The IMEI database solution should be able to enforce business rules and restrictions for one or more devices (IMEI ranges); 2.1.8.29. The software solution of the Central IMEI database must be integrated with the local IMEI database of the mobile operator (s). The Central IMEI database and the local IMEI database must be synchronized automatically in both directions from the Central IMEI database to the local IMEI database or in the other direction, should be able to list IMEI/IMSI pairs in three categories of white, black, and a minimum of 5 categories of gray list; 2.1.8.30. IMEI codes database – Compliant devices and other devices allowed to access the network freely (whitelist); 2.1.8.31. IMEI codes database – non-Compliant devices and other devices not allowed to access the network (blacklist);

	2.1.8.32. The solution must support transaction logging. Transactions required for registration should be configurable: white, black, gray (any or some variant of the extended gray list), all or any combination; 2.1.8.33. Synchronization of transaction events of the Central IMEI database in real time with local IMEI database operators; 2.1.8.34. The solution must take steps to add, delete and update the central database through a series of API (Application Interface). 2.1.8.35. The solution must take steps to add entries in one or more formats via API. In addition, the system must have an API for reading and searching in the system; 2.1.8.36. The solution must provide functions to import and export from/to the central and local databases; 2.1.8.37. The solution should provide features that allow local database recovery to occur quickly and independently of replication activity; 2.1.8.38. The solution should be able to receive the IMEI blacklist group, and those that are paired with any IMSI should be banned from service; 2.1.8.39. The solution must be able to receive IMEI whitelist groups that are allowed in pairs, with any IMSI to be provided by all operators; 2.1.8.40. The solution should be able to receive the IMSI blacklist group, and those that are paired with any IMEI should be banned from maintenance; 2.1.8.41. The solution must implement the priorities of the rules at this stage, and the overlapping rules; 2.1.8.41.1. White couple (IMEI, IMSI); 2.1.8.41.2. Black pair (IMEI, IMSI); 2.1.8.41.3. IMEI whitelist; 2.1.8.41.4. IMEI blacklist; 2.1.8.41.5. VIP IMEI, that can function normally on the system even if it’s non-compliant. The access to add VIP IMEI shall be restricted to certain users and shall be monitored by the SW to avoid fraud; 2.1.8.41.6. VIP mobile numbers, that can function on any IMEI. The access to add VIP mobile numbers shall be restricted to certain users and shall be monitored by the SW to avoid fraud;

	2.1.8.41.7. Ability to adjust the list of priorities by the Client; 2.1.8.41.8. Mobile Network Portability (MNP) support 2.1.8.42. The solution should be compatible with eSIM-enabled devices 2.1.8.43. Prioritization of rules should be reconfigurable, i.e. "rules engine". 2.1.8.44. It should be possible to provide a minimum of 5 different options of the equipment status in the grey list (grey1, grey 2 ... grey5) in the database.
2.1.9.	**EIR (Equipment Identity Register) requirements**
	2.1.9.1. Service provider shall provide his own EIR system to be installed across all operators in the country. The SW shall not rely on any third party EIR and shall replace existing ones (if any) 2.1.9.2. EIR shall be integrated with MSC, SGSN, GGSN and MME nodes of the operators 2.1.9.3. EIR shall receive MAP_V1_E(A)_ENHANCED_CHECK_IMEI or MAP_V2_ENHANCED_CHECK_IMEI and shall forward the related IMEI/IMSI/MSISDN to MDC 2.1.9.4. EIR shall receive 3GPP_ME_IDENTITY_CHECK request from MME and shall forward the related IMEI/IMSI to MDC 2.1.9.5. EIR shall provide at least the below functionalities: 2.1.9.5.1. IMSI extension; 2.1.9.5.2. IMEI-IMSI pairing; 2.1.9.5.3. Multiple list support; 2.1.9.5.4. XDR generation for each Check-IMEI operation; 2.1.9.5.5. 2G/3G/4G support 2.1.9.5.6. 1 IMEI to 1 IMSI/MSISDN lock rule 2.1.9.5.7. 1 IMEI to public IMSI/MSISDN lock rule 2.1.9.5.8. 1 IMSI/MSISDN to public IMEI lock rule 2.1.9.5.9. 1 IMEI to N IMSI/MSISDN lock rule 2.1.9.5.10. 1 IMSI/MSISDN to N IMEI lock rule 2.1.9.5.11. N IMEI to N IMSI/MSISDN lock rule
2.1.10.	**Mobile Device Compliance System External Communications**
	2.1.10.1. API interface - automatic interface through which information systems of the operators and ICASA can interact with the application processing system. Data exchange should be carried out via message and comply with security requirements; 2.1.10.2. CLI (Command Line Interface) - a mass import / export of data or provision in the GSM Association (GSMA) format;

	2.1.10.3. File Interface (SFTP) - download interface for storage and incremental updates of information on IMEI-codes of mobile client devices, and to provide the platform logs including all checkIMEI and ME-Identity-Check requests received along with their responses; 2.1.10.4. SNMP – used for alarms integration and reporting of any issue in the platform 2.1.10.5. The supplied SW must be able to use any of the interfaces at the same time and provide responses to applications on the same interface. The Supplier must provide the Client with the functionality, ability to create, configure, modify, and delete an existing number transfer process with a detailed description.
2.1.11.	**Requirements for reliability and availability**
	2.1.11.1. There must be a backup solution with primary and backup units, and the ability to automatically switch and synchronize between the primary and backup unit. A backup unit must correctly process the received data in the event of failure of the primary unit. 2.1.11.2. To ensure high availability of the main SW block, fault-tolerant mode with clustering of all components on the principle of "hot standby" should be supported; 2.1.11.3. In the event of a shutdown and further recovery, the SW should continue to process received applications correctly in automatic mode; 2.1.11.4. The solution must be available on a 24/7/365 basis. In case of critical situations and unavailability of the system, the time required to recover is not more than 3 hours; 2.1.11.5. All SW components must be reserved and must not contain a single-point failure. 2.1.11.6. All data replication between active nodes shall be in real time, with no data difference between primary and secondary nodes of the system.
2.1.12.	**Monitoring and statistics requirements**
	2.1.12.1. The SW must have built-in monitoring systems for tracking: 2.1.12.1.1. Alert notifications should be visible locally and stored in a separate alarm log. 2.1.12.1.2. Current stream of processed rules and categorization of the IMEI codes; 2.1.12.2. SW must provide as a minimum: 2.1.12.2.1. Collection and distribution of notifications based on:

	2.1.12.2.1.1. Emergency situations; 2.1.12.2.1.2. Increasing download threshold; 2.1.12.2.1.3. Interface Status Changes and software or hardware components; 2.1.12.2.1.4. Violation of the threshold for the time interval of number transmission. 2.1.12.2.2. Registration records for the following events: 2.1.12.2.2.1. Administrator and user actions with the indication of IP-addresses; 2.1.12.2.2.2. Notification of errors and malfunctions; 2.1.12.2.2.3. Control over the implementation of changes. 2.1.12.2.3. Security Audit and System Monitoring: 2.1.12.2.3.1. Monitor the system in all locations (i.e. Central System, and MNOs local System); 2.1.12.2.3.2. Identify and save any attempt to modify the data stored in the system, by any user. The system must identify the user that modified the data, the IP-address, the data modified, and the time of modification; 2.1.12.2.3.3. Send all auditing results in real time to the central database located in the central site; 2.1.12.2.3.4. Implement an alert system that will notify personnel of any security breach or data modification, in real time. 2.1.12.2.4. Reconciliation and Fraud detection 2.1.12.2.4.1. SW must detect any fraud action and take necessary measures accordingly. SW shall send alarm notification instantly upon fraud detection; 2.1.12.2.4.2. A reconciliation must be done to compare the IMEIs detected on the network with the IMEIs categorized in the central Database, in addition to reconciliation of the rules applied to the IMEIs.
2.1.13.	**Reporting Requirements**
	2.1.13.1. Real-time reporting interface that reflects the CheckIMEI and ME-Identity-Check requests received by MDC system, the response of MDC system to these requests, and the categorization of IMEIs in the system; 2.1.13.2. Interface shall include an auto refresh option to automatically load the new data and display them; 2.1.13.3. Filtering, grouping information stored in the system, and creating statistical reports;

	2.1.13.4. The ability to view reports should contain detailed information related to the IMEIs, the categorization of devices, the TPS, statistics about WL/GL/BL responses, and CheckIMEI and ME-Identity-Check requests and responses; 2.1.13.5. Other reports in accordance with the requirements of the customer and operators. Reports should be comfortable for further detailed analysis and should comprise various types of representations - tables, graphs, charts. 2.1.13.6. When requesting the report, the user shall be able to specify any "FromDate" and any "ToDate", in addition to previously defined date ranges such as "Today", "Yesterday", "This week", "Last 15 minutes", "Last 30 minutes", "Last 1 hour", etc. 2.1.13.7. Reporting section shall give the customer a clear view on the below figures: 2.1.13.7.1. GSMA approved devices; 2.1.13.7.2. Non-GSMA devices (i.e. fake IMEIs); 2.1.13.7.3. Zero IMEI devices; 2.1.13.7.4. Cloned and Duplicate IMEIs; 2.1.13.7.5. IMEI swap numbers; 2.1.13.7.6. IMSI swap numbers; 2.1.13.7.7. Detected IMEIs, IMSIs, MSISDNs on the network; 2.1.13.7.8. Blacklisted IMEIs, IMSIs, MSISDNs detected on the network; 2.1.13.7.9. Greylisted IMEIs, IMSIs, MSISDNs detected on the network; 2.1.13.8. Device distribution reports shall be provided including distribution per model, manufacturer, OS version, etc. 2.1.13.9. Subscriber list reports shall be provided including list of subscribers having a specific device model, manufacturer, etc. 2.1.13.10. Device change reports 2.1.13.11. Evolution charts

3. Period of assignment

All work is to be carried out in accordance with the timeline as agreed with the Authority. The Authority will not be responsible for any cost incurred due to an extension of the project resulting from delays by the Supplier.