DIRBS SOP 2017

PTA/DIRBS/SOP/001

Version 1.06

9th November, 2017

Amendment Date: 30th November 2018

Table of Contents

DIRBS SOP

1. Introduction

Pakistan Telecommunication Authority is empowered under section 9.6.2, 9.6.3 and 9.6.4 of the Pakistan Telecommunications Policy, 2015, to develop a regulatory framework to ensure that stolen phones, blocked phones, and phones with duplicate or non-standard identifiers are blocked from use in Pakistan. To implement the policy a regulatory framework, available on PTA website in the form of DIRBS Regulations, has been developed with the consultation of the stake holders and a Mobile Device Identification, Registration and Blocking System (DIRBS) has been developed and installed by PTA.

DIRBS will function by analyzing data dumps received from MNOs. It will generate a black list, exceptions list and notifications list. The first two lists will be implemented by MNOs on their EIRs. Implementation of the lists will result in blocking of non-compliant devices. Their implementation will also result in unblocking of recovered devices and pairing of existing non-compliant devices with SIMs of owners who are given relief by PTA.

2. Definitions.

2.1. **"Authority"** means Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunication (Re-organization) Act,1996;

2.2. **"Person"** means a natural or juristic person who intends to import PTA approved terminal equipment into Pakistan with the objective of personal use or sale of such equipment, for connection to a public switched network. (2) Words and expressions used but not defined herein shall bear the meanings given there in the Act or the Rules.

2.3. **"Black List"** means a list of IMEIs that are associated with mobile device(s) which have been denied mobile communication service(s) by Mobile Networks Operator(s) (MNO) as they have been reported lost, stolen, have an invalid IMEI number(s), have duplicate IMEI(s) or not having certification of compliance to technical standards for such mobile devices issued by the Authority;

2.4. **"Cloning"** means transfer of identity (IMEI) from one mobile device to another.

2.5. **"Compliant Mobile Device"** means a device that fulfils the following requirements:

2.5.1. Devices with valid IMEIs assigned by Global System Mobile Association(GSMA);

2.5.2. Devices with unique IMEIs;

2.5.3. Devices not in the stolen/lost lists (reported locally to the Authority and globally to GSMA); and

2.5.4. Devices type approved/having Certification of Compliance to Technical Standards for IMEI devices issued by the Authority.

2.6. **"Device Pairing System"** means creation of IMEI - Subscription paired exceptions for permission to allow non-compliant devices to keep receiving mobile service only with the subscription they are paired with

2.7. **"Device Registration System"** means a registration for certification of compliance to technical standards' for IMEI devices in the manner as prescribed by the Authority to the Persons/ Distributers/OEMs/ODM(s)/Type approval Holder(s)/Individuals from time to time;

2.8. **"Device Verification System"** means a web interface and application for stakeholders to verify mobile device status

2.9. **"Duplicate IMEI"** means IMEIs found with two or more mobile devices and also includes same IMEI on a dual or more SIM device for each SIM slot.

2.10. **"Exception List"** means a list containing specific IMEI(s) and Subscription Pairings that are allowed to continue receiving Mobile Communication Services even if their IMEI(s) appear on the blacklist on the basis prescribed by the Authority;

2.11. **"Genuine Duplicate Device"** means a device - having valid GSMA assigned IMEI – whose IMEI has been duplicated in another device(s) which does not have the same IMEI assigned to it.

2.12. **"IMEI"** means an international mobile equipment identity by GSMA and it comprises of unique 15 digit decimal numbers required to identify mobile devices on mobile networks

2.13. **"IMEI-Subscription Pairing"** means pairing of a particular IMEI with subscriber's SIM;

2.14. **"IMSI**" means the International Mobile Subscriber Identity is used to identify the user of a particular mobile network operator and is unique with all the cellular networks. IMSI consists of mobile country code, mobile network code etc.

2.15. **"Mobile Device Blocking"** means-denial of telecommunication service to a device by the MNOs

2.16. **"MSISDN**" means the Mobile Station International Subscribers Directory Number is a number uniquely identifying a subscription in a GSM or a UMTS mobile network.

2.17. **"Non-Compliant Device"** means a device which does not fulfill any condition(s) as defined for compliant devices.

2.18. **"Notification List"** means a list of Mobile Devices with certain authentication issues such as having IMEI numbers allocated by GSMA but is not type approved by PTA, and/or does not have certification of compliance to technical standards for IMEI devices issued by Authority and /or is non-duty paid and/or is duplicate IMEI and/or any other reason notified by PTA

2.19. **"OEM/ODM"** means an Orignal Equipment Manufacturer/Orignal Devise Manufacturer, who are type approval holder(s), to market and sell mobile devices in the territory of Pakistan;

2.20. **"Secure File System"** means the secure interface for Mobile Network Operators to upload mobile device data in the Authority pre-defined format;

2.21. **"Type Approval Holder"** means and includes an entity holding a valid type approval certificate issued by the Authority under the Type Approval Regulations, 2018 (as amended from time to time).

3. Implementation Phases

3.1. Phase 1. The phase consists of mapping and identification of IMEIs, including blocking of stolen/lost devices. **Phase 1 will start with effect from 10th May 2018 and will end on 30th November 2018**. Following will be done during this phase:

3.1.1. The devices (IMEIs) observed during this phase operational on MNOs networks which do not comply with clause 2.5.1 and/or 2.5.2 of this SOP will be paired with SIM (IMSI) by DIRBS as per the **clauses 10.1 and 10.2 of this SOP**.

3.1.2. For phase 1 only, IMEI devices conforming to conditions 2.5.1, 2.5.2 & 2.5.3 of the given "compliant devices" definition will be considered valid after analysis done by PTA**.**

3.1.3. Black list containing IMEIs of stolen/lost devices will be generated by DIRBS and provided to MNOs on daily (working days) basis for implementation on EIRs for blocking. Subsets of black list will also be provided as per clause 6.1.9 of this SOP.

3.1.4. Exception and Notification lists will be populated by DIRBS but will not be implemented on EIRs by MNOs during Phase 1. However, these lists will be provided to MNOs for their information.

3.1.5. Updated Exception and Notification lists will be provided to MNOs twice a month by DIRBS. However PTA may change the provision of these lists as and when required.

3.1.6. Black list will be common for all MNOs, whereas Exception and Notification lists will be operator specific.

3.1.7. SMS Messages will be sent to users, whose IMEI-IMSI pairings are included in the Exception List, by DIRBS core through SMSCs of relevant MNOs. Table of reasons for pairing and the relevant messages (Non-Compliant Device Possibilities, Reasons and Messages) is attached as Appendix A.

3.1.8. The contents and format of the Black, Exception and Notification lists are attached as Appendix B.

3.1.9. Before the end of Phase 1 or as decided by PTA, DIRBS will provide a list of all IMEIs observed on the MNO Networks to PTA, which conform to clause 3.1.2 above. PTA will validate the list and subject to fulfilment of other requirements of a compliant device, these IMEIs will not be included in the Black lists generated during Phase 2.

3.1.10. All paired devices during phase 1 will be allowed to continue receiving cellular services till the expiry of their useful life.

3.1.11. All Mobile Devices already active on Cellular Mobile networks within Pakistan till 1st December, 2018 will remain operational without service disruption. Even non-compliant devices in operation before this date will be tied to those numbers and will remain operational till the useful life of the device.

3.2. Phase 2. Full blocking to be supported including blocking of non-compliant devices except those paired in accordance with clause 3.1.1.All the valid IMEIs which were not observed during Phase 1 and start appearing during Phase 2 will have to get type approval and/or certificate of compliance from PTA.

3.2.1. **Phase 2 will start on 1st December 2018.**

3.2.2. **MNOs system must be ready in terms of hardware and software in order to support DIRBS system by 10th October 2018 so that their testing can be carried out between DIRBS and MNOs EIRs before launch of phase 2.**

3.2.3. MNOs have to make sure that they have implemented the final Exception list of Phase 1 before starting the Phase 2.

3.2.4. During this Phase black list will consist of IMEIs of all the non-compliant devices and the IMEIs of devices on the exception list, less the IMEIs of devices specified in clause 3.1.9 above.

3.2.5. Each non-compliant device (operational on the Networks) will be sent message by DIRBS through relevant MNO SMSC informing him that the device is noncompliant, the reason of non-compliance and that it will be blocked after 15 days of the message sent to him if discrepancies are not removed. The message will also guide the user to visit DIRBS portal for information on how to get the device regularized from PTA.

3.2.6. MNOs will ensure that they implement blacklist and exception list on their EIRs as and when provided by the PTA.

3.2.7. Updated Black list will be provided on daily (working days) basis, whereas other two lists will be provided twice a month. However, the frequency of provision of Exception and Notification lists may increase or decrease if required by PTA. Subsets of black list and exception list will also be provided as per **clause 6.1.9 and 6.2.7 of this SOP.**

3.2.8. Each MNO will ensure that the latest updated lists have been implemented on the EIRs at all times.

3.2.9. As a result of implementation of lists on EIRs, IMEIs in the Black list will be blocked except those which are in the Exception list.

3.2.10. The devices whose IMEIs are in the Exception list will work only with the SIMs whose IMSIs have been paired with the IMEI still expiry of useful life of the device(s).

3.2.11. Call flow required for DIRBS exception list support in MNO network will be as given in Appendix C.

3.2.12. Service based (RAT field) clone detection will be used to curb IMEI duplication by PTA (DIRBS).

3.2.13. All the duplicated IMEIs having valid GSMA IMEI will be notified to provide proof of authenticity of their device. IMSI(s) of Genuine Duplicate Device will be paired after providing proof to PTA and the IMEI will be added to the black list.

3.2.14. PTA will differentiate between a genuine duplicate device and a non-genuine duplicate device in accordance with clause 15.

3.2.15. The paired devices will continue to receive service till expiry of the useful life of the device(s).

4. International Roamers

4.1. Roamers will be allowed service while roaming in Pakistan in accordance with Regulation 8 of DIRBS Regulations.

4.2. Roamers will be allowed service for unlimited period, however, the Authority retains the right to revise the time limit to a finite time period.

4.3. In case of finite time limit, change in IMSI or IMEI will not reset the Roaming Period to initial value.

4.4. If a roamer starts using local SIM his/her device, he/she will not be considered as a roamer and will be required to fulfill the conditions of a compliant device as per clause 2.5 of this SOP. Individual whose devices are deficient of the condition 2.5.4 only, may obtain certificate of compliance to technical standards for IMEI based devices from PTA through Device Registration System (clause 8.1) by following the procedure given in Appendix E to this SOP for individuals travelling e.g. aero-plane, ship, border crossing etc.

4.5. If an international roamer has device with dual or more SIM slots his handset will continue to function without hindrance, however if he inserts local SIM(s) into any of the slots the IMEI of that slot will be blocked if it does not conform to the conditions of compliant device given in clause 2.5.

4.6. If the international visitor inserts local SIM and his device is non-compliant he/she will be intimated the reasons of non-compliance along with necessary actions required for continuity of service(s) through SMS by DIRBS. Failure to do so will result in blocking of device after the SMS notification expiry of 30 days. Before blocking device user will be notified along with reasons through SMS.

5. Data Dumps Uploading by MNOs

5.1. All MNOs shall upload Data dumps to DIRBS servers, through secure connectivity between DIRBS and each MNO, as per the requirements/format attached as Appendix D.

5.2. Data dumps will consists of DATE, IMEI, IMSI, MSISDN and RAT columns in the format attached at Appendix-D.

5.3. Before uploading the data dumps, MNOs shall validate the dumps through the latest version of validator provided by PTA.

5.4. MNOs shall upload the validated data dumps for the second half of previous month between every 1st to 3rd of next month and for the first half of current month between 16th to 18th of that month. The timelines for provision of data dumps will be revised as and when required by the Authority.

5.5. Secure IT connectivity for uploading of data dumps of their respective networks will be established/maintained by each MNO with DIRBS.

5.6. On receipt of data dumps by the system the data will again be validated and processed. In case any discrepancy is found in data dumps, the system will generate and transmit a notification to the relevant MNO. Data dumps will be provided again by the MNO with updated version number with in next 24 hours.

5.7. Each MNO shall make it ensure that data dumps shall be uploaded (pushed) to the DIRBS server in accordance with the schedule at clause 5.4 above. MNOs shall nominate the focal person in case of any problem arise for collection of data dumps through IT connectivity between DIRBS and MNOs in order to resolve the issue.

6. Handling of DIRBS Lists

6.1. Black List

6.1.1. It will be prepared as per the format prescribed in Appendix B.

6.1.2. It will be generated by DIRBS on daily basis (working days).

6.1.3. During Phase 1 it will consist of IMEIs of stolen/lost mobile devices

6.1.4. During Phase 2 it will consist of IMEIs of all the non-compliant devices and the IMEIs of devices on the exception list, less the IMEIs of devices specified in clause 3.1.7 above.

6.1.5. It will also contain IMEIs of exception lists

6.1.6. MNOs will implement the list on their EIRs within 24 hours on receipt from PTA.

6.1.7. It will be transmitted to MNOs over IT links by using secure file system for uploading data for implementation within their EIRs.

6.1.8. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading list.

6.1.9. For practical implementation reasons Sub-sets of blacklist in the form of daily add and remove lists will also be provided to each MNO.

6.1.10. To ensure all implemented Black lists are synchronized with DIRBS Black list PTA may require MNOs to provide copy of the Black lists implemented in their EIRs from time to time.

6.2. Exceptions List

6.2.1. It will be prepared as per the format prescribed in Appendix B.

6.2.2. Exception list will consist of all the IMEI-IMSI pairings/re-pairings done in accordance with clause 10 below

6.2.3. It will be generated by the system twice a month initially. The Authority may revise it from time to time.

6.2.4. It will be implemented by MNOs on EIRs in Phase 2 within 24 hours on receipt from PTA.

6.2.5. It will be transmitted to MNOs over IT links by using secure file system for uploading data and its implementation on their EIRs.

6.2.6. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading the list.

6.2.7. For practical implementation reasons Sub-sets of relevant Exception list in the form add and remove lists will also be provided to each MNO during phase 2.

6.2.8. To ensure all implemented Exception lists are synchronized with DIRBS Exception lists PTA may require MNOs to provide copy of the Exception lists (through IT link) implemented in their EIRs from time to time.

6.3. Notifications List

6.3.1. Notification list will consist of IMEIs, IMSIs, MSISDNs, Block dates and reasons of IMEIs being on notification list.

6.3.2. DIRBS will intimate the consumers through SMS about their device(s) status as specified in clause 3.1.5 above.

6.3.3. Notification List will be prepared as per the format prescribed in Appendix B.

6.3.4. It will be generated by DIRBS twice a month initially. The Authority may revise the frequency from time to time.

6.3.5. It will be sent to MNOs for information regarding their consumer being notified.

6.3.6. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading the list.

7. Other Inputs to DIRBS

7.1. Multiple Lists are inputs to DIRBS in CSV format which are Stolen/lost, GSMA TAC and devices having certificate of compliance to technical standards issued by the Authority.

7.2. Lists will be transmitted to MNOs through SFTP.

7.3. Stolen Phone List.

7.3.1. Reported stolen/lost/recovered devices' IMEIs will be included/removed in/from black list on daily (working days) basis.

7.3.2. Existing, complaint registration procedure of stolen/lost devices and handling of found/recovered devices by PTA will continue as given in Appendix H, except that block and unblock lists will be provided to DIRBS instead of MNOs.

7.3.3. After sufficient experience or as decided by PTA the process of complaint registering for blocking/unblocking of stolen mobile devices to PTA and eventual blocking/unblocking intimation to DIRBs will be automated through DIRBS Web Portal and/or mobile app and or any other available means.

7.4. GSMA TAC Numbers List**.** Latest GSMA TAC number lists will be uploaded in the system on occurrence

7.5. Certification of Compliance to Technical Standards for IMEI Based Devices Updates**.** Device Registration System (DRS) will be populated with the details of devices which have been issued the certification (commercial/personal) by PTA till date and kept updated from there on.

8. DIRBS Subsystems

8.1. Device Registration System (DRS)**.**

8.1.1. DRS will be a web based system, provided by PTA, designed to facilitate Type Approval Holders/Authorized Distributers/OEM/MNOs/Individuals to apply for issuance of Certification of Compliance to Technical Standards for IMEI devices to PTA.

8.1.2. After the issuance of Certificate of compliance to technical standards to the applicant by PTA, DRS will upload the data to the DIRBS system.

8.1.3. Role Based Access Levels are listed as Appendix-E.

8.1.4. Procedure for obtaining Certificate of Compliance to Technical Standards for IMEI Based Devices by commercial entities and individuals is attached as Appendix G.

8.2. Device Verification System (DVS)**.**

8.2.1. DVS will be a web/mobile app/SMS based system, provided by PTA, for general public through which they will be able to verify the validity/legality of an IMEI/Device.

8.2.2. The SMS facility will be provided via the SMSC of MNOs at their own cost for public facilitation through Large Account and it will not be charged for outgoing SMS. However the mobile operators may charge their customers a maximum sum of Paisa 10 + tax per SMS query.

8.2.3. Role Based Access Levels are listed as Appendix-F

8.3. Secure File System (SFS)**.**

8.3.1. Secure File System will be used to upload data dumps by MNOs to DIRBS and to transfer the three lists which include blacklist, exception list and notification list to MNOs by DIRBS.

8.3.2. The Files will be transferred using SFTP.

8.4. SMS/Notifications Generation System**.**

8.4.1. Each MNO will establish connectivity between DIRBS core and its SMSC for generation of SMS messages to subscribers as per notifications list and to respond to users' SMS messages for verification of IMEIs. It will send SMS to consumers using MNO SMSC.

8.4.2. DIRBS will ensure that no bulk messages are broadcasted during peak hours.

8.4.3. DIRBS SMSC servers will be connected to all MNOs through SMPP protocol.

8.4.4. SMSC connectivity will be arranged by each MNO and provide relevant SMSC documentation to integrate with DIRBS SMS gateway.

8.4.5. SMS throughput will be ensured by MNO to avoid SMS congestion.

9. DIRBS – MNOs Connectivity

9.1. Redundant Point to Point secure connectivity will be arranged by MNOs to DIRBS.

9.2. 99.9% connectivity uptime will be ensured by MNO/Service providers.

9.3. Each MNO shall designate responsible representative to ensure connectivity to the System.

9.4. Connectivity requirement throughput is 20 Mbps. Requirement may be revised as and when required by PTA.

9.5. IT connectivity as per clause 9.1 of this SOP will be used to send/receive SMS notification to consumers, Uploading of Data Dumps by MNOs to DIRBS and Downloading of DIRBS Lists by MNOs.

10. Pairing/Re-pairing

10.1. During Phase 1, all non-compliant device IMEIs which do not have valid IMEIs or are not unique will be paired with all the SIM(s) (IMSI(s)) in use with these devices subject to clause 10.6 below.

10.2. Pairings mentioned in clause 10.1 will be done automatically by DIRBS and will remain paired for the period given in clause 3.1.10 above.

10.3. During Phase 2, only genuine duplicated IMEIs will be paired after providing proof to PTA and the IMEI will be added into the black list.

10.4. During Phase 2, paired devices will be eligible for pairing with another SIM (IMSI) under the following conditions;

10.4.1. SIM damaged or lost provided there is no MSISDN change

10.4.2. SIM changed due to conversion from a previous generation technology to a next generation technology e.g. from 3G to 4G etc. provided there is no MSISDN change.

10.4.3. A genuine duplicated device user wants to sell/gift the device will be allowed to re-pair the IMSI of new owner with the IMEI of the device.

10.4.4. Any other conditioned notified by PTA

10.5. During Phase 2 Mobile Number Portability (MNP) for paired devices will not be allowed

10.6. Each IMSI/MSISDN can be paired with maximum 10 non-complaint IMEIs except unique stolen/lost IMEIs which will be handled by DIRBS.

11. Continuity of Service to Paired Devices on SIM Change

11.1. To ensure minimum disruption of service MNOs may replace the IMSI of the relevant IMEI-IMSI pair in their EIRs for the situations mentioned in Clause 10.4.1 and 10.4.2 above.

11.2. MNOs will report to PTA for each occurrence through DIRBS portal.

11.3. For the situation mentioned in clause 10.4.3 request will be sent to DIRBS through web portal by the selling owner to change his/her pairing by providing seller's and buyer's MSISDNs and their service providers. DIRBS will identify the IMSI of the seller and obtain IMSI of buyer from his service provider.

11.4. DIRBS will amend the exception lists of both MNOs unpair/re-pair the old/new IMSIs with the device IMEI and send the add/remove sub-sets of the exception list(s) to MNO(s) concerned for implementation. The change will take affect in 48 to 72 hours

11.5. MNOs will not include any additional IMEI-IMSI combination into the exception list of their system not covered under clause 10 of this SOP.

12. EIR Upgradation

Cellular Mobile operators shall upgrade their systems in terms of hardware and software to support Exception and Black lists of DIRBS system in the following manners.

12.1. MNOs will upgrade their EIR to accommodate both Valid & Invalid IMEIs in Black List.

12.2. Mobile Operators will upgrade their EIR to accommodate Exception List.

12.3. In Exception List, there must be a pairing of IMEI with IMSI. The overall customization of EIR shall be completed as per PTA decision

12.4. The capacity of Black list & Exception list maintained by operators must be sufficient to accommodate existing subscriber as well future forecast.

12.5. Any future Software & Hardware expansion requirements of EIR, must be catered by MNOs.

12.6. All MNOs will customize their EIRs to convert NULL IMEIs to 14-digit ZEROs, 1s, 2s up to 9s or any other sequence or as required by PTA.

13. Removal of an IMEI from the Black List

13.1. A blacklisted device will not be activated except for lost/stolen devices which have been found/recovered and type approved devices/Issued certification of Compliance to technical standards for IMEI devices or as required by PTA.

13.2. Unblock list of found/recovered devices will be provided as per clause 7.3.3 above to DIRBS.

13.3. Unblock lists of Type Approved devices will be provided to DIRBS, in accordance with clause 8.1.2 above.

13.4. The provision of unblocking lists vide clauses 13.2 and 13.3 above to DIRBS will result into automatic removal of the relevant IMEIs from the black list, which on implantation by MNOs on their EIRs will result in unblocking of the IMEIs provided vide clauses 13.2 and 13.3

14. Customer Services

14.1. PTA will provide relevant information to the public through awareness campaign before the launch of DIRBS and through DIRBS portal accessible through PTA web site. There will be no direct contact by the customers with PTA except where specifically indicated in this SoP.

14.2. Complaints by customers will be handled in accordance with DIRBS Regulation 18

14.3. All MNOs/Type Approval Holders/Distributors/Persons will train their Customer Service Center/Help line agents to handle DIRBS related queries/complaints by the customers.

14.4. Apart from any other relevant information the agents will be trained so that they are familiar with the contents of Appendix A, Device Verification System (Clause 8.2 above) and Device Registration System for individuals (Clause 8.1 above) so that they can guide the complainants appropriately

14.5. To train the agents, train the trainer programs will be arranged by DIRBS team at 2-3 location in consultation with MNOs.

14.6. DIRBS will provide Device Verification System for the public to verify the compliance status of IMEIs. The facility for checking will be provided on DIRBS portal, DVS App and SMS short code.

14.7. For SMS query customers may be charged as per clause 8.2.2 above

14.8. Existing stolen/lost mobile phone procedure will be as given in clause 7.3 above and explained in detail in Appendix H.

14.9. Genuine device whose IMEI has been duplicated will be handled in accordance with clause 3.2.13 above and DIRBS Regulation 13(2).

15. Handling of Genuine Duplicate Devices

The following criteria shall be used to address if a duplicate IMEI device is Genuine Duplicate Device or otherwise.

15.1. On detection of duplicated IMEIs in Phase 2 the owners for duplicated IMEI devices(s) will be notified through SMS by DIRBS and his device is non-compliant he/she will be intimated the reasons of non-compliance along with necessary actions required for continuity of service(s). Failure to do so will result in blocking of device after the SMS notification expiry of 15 days. To avoid blocking they would be directed to provide following documents through DIRBS web portal for evaluation by PTA:

15.1.1. CNIC/Passport

15.1.2. Original purchase invoice

15.1.3. Original warranty card.

15.1.4. Any other document available to prove ownership

15.1.5. Images of the mobile device and its original box under investigation

15.2. After receiving user provided documentation through DIRBS web portal, it will be co-related with extracted data from DIRBS. The same will be evaluated for authentication of mobile device IMEI.

15.2.1. All MSISDNs and IMSIs used with the IMEI along with dates of usage

15.2.2. Device type i.e. 2G, 3G,4G on future supported technologies device

15.2.3. Which service(s) (2G, 3G or 4G) accessed by the IMEI along with the each MSISDN.

15.3. With the information available vide clauses 15.1 and 15.2 it will be possible to distinguish between the genuine and non-genuine duplicate devices.

15.4. If required the PTA may ask the owners to bring the devices/boxes/documents for physical inspection.

15.5. After evaluation, if it is observerd that the mobile device having genuine IMEI number and its duplicate IMEI is being paired in Phase 1. Such handset will be paired and the IMEI will be added into the black list.

16. Coordination. For smooth functioning of DIRBS, all MNOs, DIRBS, Type approval holders / distributors/persons and PTA will nominate Points of Contact PoCs.

17. The said SOP shall be revised in consultation with all stake holders by the authority.

Appendix A

Non-Compliant Device Possibilities, Reasons and Messages

In line with the definition of a compliant device, following conditions may occur for compliant/noncompliant devices. Any other combinations are invalid combinations.

ISSUES				TREATMENT & MESSAGES				
GSMA Invalid	Stolen	Duplicate	No COC	Phase 1		Phase 2		
							Observed First Time	Observed in Phase 1
				C	Your mobile device IMEI is compliant (PTA Approved)	C	Your mobile device IMEI is compliant (PTA Approved)	Your mobile device IMEI is compliant (PTA Approved)
			*	V	Your device IMEI is Valid. If you haven't used this device then insert SIM and make a call/SMS to anyone for auto registration	N	Your device IMEI is non-compliant.	Your mobile device IMEI is compliant (PTA Approved)
		*		P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	P (Genuine only)	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.
		*	*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	N, P (Genuine only)	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.
	*			B	Device IMEI is blocked. Reported stolen	B	Device IMEI is blocked. Reported stolen	
	*		*	B	Device IMEI is blocked. Reported stolen	B	Device IMEI is blocked. Reported stolen	
*				P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	B	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.
*			*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	B	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.
*		*		P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	B	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.
*		*	*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continuous receiving services.	B	Your device IMEI is non-compliant.	Device IMEI is non-compliant. Your IMEI has been paired with your mobile number (MSISDN) and your device will continuous receiving services.

Treatment Legends	
Block	B
Pair	P
PTA Certification of Compliance Required	N
Validated by PTA	V
Compliant	C

Contents and Format of Black, Exception and Notification Lists

1. Lists will be shared using secure FTP and authorized credentials. Lists will be in .CSV format. Size of each list is dependent on project implementation phases.

2. Date and time will be appended in name of list after consultation with stakeholders e.g black_list_20172509.csv

3. Frequency of lists will be as follows:

List Name	Distribution Frequency
Black List	Daily
Notification List	(Currently after 15 days)
Exception List	(Currently after 15 days)

4. Black List Sample:

   a. Black list will be same for all operators

   b. Headers are (IMEI, BLOCK_DATE, REASONS)

   c. List will not be delta list

   d. Sample entries are given below:

Imei	block_date	reasons
35335407509863	20170701	Stolen
35551405663500	20170701	Stolen
35396801210014	20170701	Stolen

5. Notification List Sample:

   a. For each operator, separate list will be provided

   b. Headers are (IMEI, IMSI, MSISDN, BLOCK_DATE, REASONS)

   c. Name of operator will be suffix. e.g, Notification_mobilink.csv

   d. Sample entries are given below:

Imei	imsi	msisdn	block_date	reasons
35738006070489	410018937826633	923084248572	20180701	Stolen, gsma_not_found, Duplicate, etc
35645606474058	410018308077873	923014772876	20180701	Stolen, gsma_not_found, Duplicate, etc
35422706411153	410018558561776	923012842203	20180701	Stolen, gsma_not_found, Duplicate, etc
35635105791242	410018138639138	923004018004	20180701	Stolen, gsma_not_found, Duplicate, etc

6. Exception List Sample:

   a. For each operator, separate list will be provided

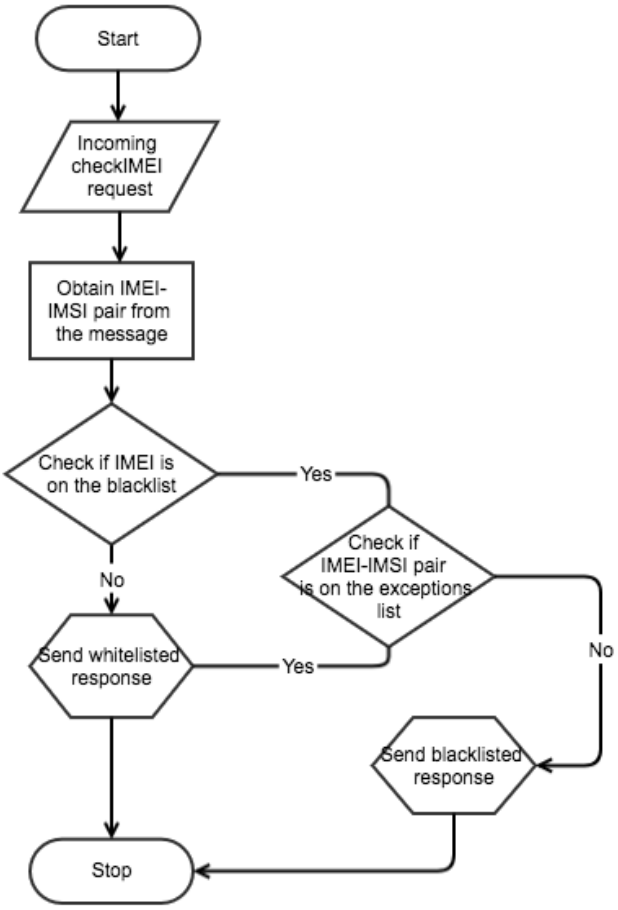
b. Headers are (IMEI, IMSI). Name of operator will be suffix. e.g., mobilink_exception.csv

c. Sample entries are given below:

Imei	Imsi
35738006070489	410018937826633
35645606474058	410018308077873
35422706411153	410018558561776
35635105791242	410018138639138

Call Flow Required for DIRBS Exception List Support

The diagram below shows the EIR call flow required for DIRBS exception list support. The check IMEI request must support both IMEI and IMSI in the check IMEI message.



Appendix D

Requirements & Format for Data Dumps

Definition of data fields

All necessary fields are available from output CDRs. Field details and formatting are shown below.

Field	CDR source fields that contain the information	Format
Date	• Converted from date portion of the following, aggregatedby localtime: o Seizure Time / Answer Time (Record Types 0, 1, 87) *(note: Seizure Time is used for unsuccessful calls, Answer Time is used for successful calls. Use Answer Time if available, otherwise SeizureTime.)* o Event Timestamp (Record Types 6-7, 21-23, 25, 28, 93-94, and IMEI ObservationTicket) o Record Opening Time (Record Types 18, 20, 84-85,96)	YYYYMMDD* (e.g. 20160423) *aggregated by local time
IMEI	• "ServedIMEI"	14-16 digits* (e.g. 013845000153547) *includes any leading zeros *(i.e. if an IMEI starts with one or more zero digits, these leading zeroes must not be stripped off, as doing so would completely change the IMEI value)*
IMSI	• "Originator IMSI" (Record Type 93) or "RecipientIMSI" (Record Type94) • "Served IMSI"(otherwise)	14-15 digits
MSISDN	• "Originator MSISDN" (Record Type 93) or "Recipient MSISDN" (Record Type94) • "Served MSISDN"(otherwise)	Up to 15 digits* (e.g. 18583551234) *in E.164 format *(i.e. international telephone number, including country code but excluding any international call prefixes*
RAT	• "System Type" (Record Types 0-1, 6-7, 23,25) □5)□□□□□□□□□□□□(Record Types 18, 20-22, 28, 84-85, 93-94, 96) *At the time of writing, defined RAT values include:* *001 – UTRAN (3G)* *002 – GERAN (2G)* *003 – WLAN* *004 – GAN* *005 – HSPA Evolution (3.5G)* *006 – E-UTRAN (4G)* *007 – Virtual* *101 – IEEE 802.16 (WiMAX)* *102 – 3GPP2 eHRPD (3.5G)* *103 – 3GPP2 HRPD (3G)* *104 – 3GPP2 1xRTT (2G)* *105 – 3GPP2 UMB (4G)*	Pipe-separated list of 3 digit codes, with leading zeroes intact

Data can be sourced from different fields in different types of CDRs produced in the operator's network (e.g. SMS, packet data, voice call, etc.…). The description in the second column in the above table is intended to identify which field in each of the possible CDR types (identified by 3GPP Record Type value) contains the relevant information.

The intention with listing many different record types is to obtain a complete view, capturing as many IMEIs as possible, regardless of the kind of chargeable activity in which they engaged. Once data is aggregated, the different source record types and fields that were used will not be apparent.

Excluded CDRs

In general, multiple CDR Record Types are intended to contribute to the final MNO data dump, as indicatedinthetableabove.However,someCDRsmaybegeneratedforIMEIsthatareinfactblockedby the EIR. If these are included by the MNO, they may appear incorrectly as "blacklist violations" (activity bydeviceswhichshouldhavebeenblocked)insubsequentreporting.Instead,thefollowingcasesshould be excluded from the file submitted toDIRBS:

Emergencycalls: Emergencycallsareallowedregardlessofblackliststatus.Theymaybeidentifiedbythe "EmergencyCalls"teleserviceinthe"Basicservice"fieldofaMobileOriginatedCallorMSC-SRVCCRecord (see 3GPP TS 32.250), or "IMSI Unauthenticated Flag" in PS CDR (see 3GPP TS32.251)

CDRs for attempts blocked by the EIR: In case a CDR is generated for an attempt by a UE that is actually unsuccessful due to EIR blacklisting. Such records may be identified by "Illegal Equipment" in the Diagnosticsfield,orbycorrelationwiththeassociatedblacklisted"IMEIObservation"ticketusingtheCall Reference field (see 3GPP TS32.250)

Aggregation of data from CDRs

Each row in an operator data dump represents an aggregation of CDR fields comprising a distinct Date-IMEI-IMSI-MSISDN combination along with a list of distinct RAT values used by that combination. This list of distinct RAT values will be pipe delimited (i.e. a concatenated list of values with each value separated by a pipe ('|') character). Blank/missing fields shall be considered as distinct values and included as such.

Below is a set of example fields before aggregation:

Date	IMEI	IMSI	MSISDN	RAT
20160130	35780502398494	310150123456789	18585551234	001
20160130	35780502398494	310150123456789	18585551234	002
20160130	35780502398494	310150123456789	18585551234	006
20160130		310150123456789	18585551234	001
20160131	35780502398494	310150123456789	18585551234	001
20160131	35780502398494	310150123456789	18585551234	002
20160131	35780502398494	310150123456790		001
20160131	35780502398494	310150123456790		001

Based on these example fields, the following would be the data dump rows created after aggregation:

Date	IMEI	IMSI	MSISDN	RAT
20160130	35780502398494	310150123456789	18585551234	001|002|006
20160130		310150123456789	18585551234	001
20160131	35780502398494	310150123456789	18585551234	001|002
20160131	35780502398494	310150123456790		001

Export of aggregated data to CSV

Data shall be exported to a CSV text file using UTF-8 character encoding. To ensure correct import, a header line shall be included in the CSV that identifies the fields being provided. Each record (including theheaderline)shallbelocatedonaseparatelinewithaCR/LFending(/r/n).Datafieldsineachlineshall be separated by a comma character. For more information on CSV format, see www.ietf.org/rfc/rfc4180.txt. Below is example CSV formatteddata.

```
Date,IMEI,IMSI,MSISDN,RAT
20160130,35780502398494,310150123456789,18585551234,001|002|006
20160130,,310150123456789,18585551234,001
20160131,35780502398494,310150123456789,18585551234,001|002
20160131,35780502398494,310150123456790,,001
```

Transfer of data to DIRBS

EachoperatorshallsecurelyuploaddatatoDIRBSduringtheirassignedtimewindowusingtheirprovided credentials. Time windows and credentials shall be provided to each operator by the DIRBS operational entity for thatcountry.

Prior to upload, operators should validate their data format using the provided schema and open source tool (identified in the schema). Performing this validation step can help ensure successful processing of the data and cut down on roundtrips.

Files transferred by each operator shall be zipped to provide efficient transfer and enable detection of corruption due to network connection failures. ZIP file details are shown below.

ZIP file name	The ZIP filename shall comprise the operator name followed by start and end dates in YYYYMMDD format as shown below. The dates shall be in local time and shall define the date range for the data inclusively (i.e. data in the file shall include both start and end dates): **OperatorName_*OptionalRegion*_StartDate_EndDate.zip** *(e.g. Foo Wireless_Zone4_20160101_20160131.zip)*
ZIP file contents	Each ZIP file shall contain only one CSV file. With the exception of the file extension, the CSV filename shall be the same as the ZIP filename as shown below: **OperatorName_*OptionalRegion*_StartDate_EndDate.csv** *(e.g. Foo Wireless_Zone4_20160101_20160131.csv)*
File security	Files shall not contain passwords. File security is accomplished via secure file transfer. No encryption is applied to files during storage on DIRBS.

Once received, each file is moved to the incoming folder in that operator's home directory on DIRBS for import and processing.

Validation of data by DIRBS

DIRBS regularly monitors for newly uploaded data from operators. When a new file is detected, it will be validated by DIRBS. If validation fails, an alert will be generated and the DIRBS operational entity for that country will contact the operator to initiate re-upload of a valid data file.

Note that while schema validation can be checked by an operator prior to upload, such validation is only asubsetofthevalidationperformedbyDIRBS,whichmayincludecomparisonagainsthistoricalmetadata, identification of invalid rows, flagging of discrepancies, and application of import failure thresholds.
Validationissuesmaybeincludedinoperatorand/orauditreportingandmayresultinavalidationfailure alert, depending on the type and/or severity of suchissues.

Appendix-E

Role Based Access Levels of DRS

Roles of DRS are as following:

User	Role	Permissions							
		View Stats	**View Logs**	**Manage Users**	**Add TAC**	**Add/ Apply COC**	**Verify COC**	**Issue COC**	**View COC**
System Administrator	**Admin**	All	All	All	Yes	Yes	Yes	Yes	Yes
Head of TA Department	**hq_Admin**	All	User activity logs	HQ_Staff, TA_Holder, Regional_Admin	Yes	Yes	Yes	Yes	Yes
TA Department Staff	**hq_Staff**	All	No	No	Yes	Yes	Yes	No	Yes
Regional Head	**regional_admin**	Regional Only	Regional user logs	Regional Staff	No	No	Yes (regional specific)	Yes (regional specific)	Yes (regional specific)
Regional Staff	**regional_staff**	Regional Only	No	No	No	No	Yes (regional specific)	Yes	Yes (regional specific)
Pakistan Customs	**customs_staff**	No	No	No	No	No	No	Yes	Yes
TA Holder	**ta_holder**	No	No	Applicant (authorized dealer)	No	Yes	No	No	Yes
Authorized Dealer	**Applicant**	No	Yes	No	No	Yes	No	No	Yes

Appendix F

Role Based Access Levels of DVS

Roles of DVS (WebApp and Mobile App) are as follows:

User	**Role**	**Permissions**	**View Stats**	**View Logs**	**View Reports**	**Query for IMEI**	**View seen_with Data**
Super Admin	System Administrator	Full System	Yes	Yes	Yes	Yes	Yes
PTA User	PTA-User	Full System Except Super Admin	Yes	Yes	Yes	Yes	Yes
MNO	DIRBS-Report DIRBS-API	Read Only	No	No	Yes (In Later Stage, currently Through SFTP)	Yes	No
Retailer/ End-Customer	DIRBS-API	Read Only	No	No	No	Yes	No

Appendix-G

Device Registration System (DRS) Procedure for Obtaining Certificate of Compliance to Technical Standards for IMEI Based Devices for Individual Entities for up to 5 Devices in a year

Appendix G-1

Standard Operating Procedure for Issuance of Certification of Compliance to Technical Standards for Mobile Devices with SIM Functionality for Personal Use/Gift etc.

1. **Background**: Individual(s) can bring upto 5 mobile devices in a calendar year for personal use, however they will be required to obtain certificate of compliance (CoC) to technical standards and IMEI which meet the codal requirements will be allowed for connectivity with mobile networks within Pakistan.

2. In order to effectively and efficiently process the cases of Certification of Compliance to Technical Standards and facilitate the general public in acquiring Certification of Compliance to Technical Standards following procedures are listed for all concerned:

(a) **For SIM/IMEI based Terminal device(s) imported by individual(s) for personal use following conditions are applicable:**

Parameter	Details
GSMA Type Allocation Code (TAC)	IMEI for device(s) will contain only GSMA TAC
Duplicated/Cloned/Stolen/Counterfeit IMEI	Mobile devices that contain duplicated/cloned/stolen/counterfeit shall not be allowed for issuance of CoC by PTA
Quantity	Only 5 mobile devices in a year will be allowed
Apply via PTA online Portal	Applicant shall apply via PTA online portal link available at dirbs.pta.gov.pk/drs and upload all listed requirement into the portal system

a. Obtain IMEI of your device using following methods prior to traveling and note it down for registration with the Customs Authority:

   i. Dial *#06# from the dial pad of your device and note down each 15-digit IMEI (for dual SIM devices) supported by the device.

   ii. IMEI is printed on the device box.

   iii. IMEI printed on the device by removing the back cover/ battery.

b. For availing registration at Arrival Airport using Customs kiosk, submit each 15 digist IMEI number of mobile device, CNIC/ Passport/ NICOP

number (whichever applicable) at Custom Desk/KIOSK. After fulfilment of codal requirements CoC will be issued.

c. For availing registration via PTA online portal system for mobile devices brought as Gift/Use via postal and courier services etc. applicant will be required to sign up at PTA websit https://dirbs.pta.gov.pk/drs and upload all listed doucments

   i. CNIC/Passport Copy of Applicant whose shipment has arrived
   ii. Custom/Courier Notice Copy showing details e.g. name of person whose name shipment has arrived, location where consignment is detained etc.
   iii. 15- digit IMEI number for Mobile Device(s)

After verification of IMEIs, ***Certification of Compliance to Technical Standards for a maximum of 5 devices**** *will be issued.*

Appendix G-2

Standard Operating Procedure for Issuance of Certification of Compliance to Technical Standards for Mobile Phones/Tablet PCs for Personal use/Gift process for PTA Zonal offices Issuance of Personal Certification of Compliance to Technical Standards through online portal

1. **Procedure for acquiring of Certification of Compliance to Technical Standards from zonal offices**
    a. **Problem Statement**
        i. Applicant residing in remote/rural areas lack awareness and are unable to apply via online portal.
        ii. Certification of Compliance to Technical Standards dispatched at remote/ rural location often are returned back by postal services due to incorrect/ hard to understand address resulting in delay for shipment release/demurrages
        iii. Often applicants request collection of Certification of Compliance to Technical Standards from PTA office within their locality to reduce postal service time, however since in-person collection service is available at PTA HQ, the applicants are unable to utilize this option
    b. **Way Forward:** In order to address the above stated problem following is proposed
        i. Delegation of Personal Certification of Compliance to Technical Standards processing via online portal system at zonal level to facilitate applicants residing within the zones/ reducing travel time of applicant to PTA HQ.
        ii. Each zone will be provided a user name and password for accessing/processing of personal Certification of Compliance to Technical Standards for the specific zone
        iii. Centralize monitoring for processed application to be done by type approval directorate
        iv. Weekly GSMA database will be uploaded through online portalby type approval directorate to ensure latest IMEI cades are available as part of IMEI verification
        v. A training session will be done with assigned zonal officer on processing/issuance of Certification of Compliance to Technical Standards

2. SOP to be followed for processing of Personal Certification of Compliance to Technical Standards using online portal at Zonal offices

1) Applicants are required to apply online or zonal officer to apply on behalf of applicant and enter all applicant credential
2) After verification of IMEIs, Certification of Compliance to Technical Standards for a maximum of 5 devices including mobile phones and tablet PCs will be issued.
3) If Certification of Compliance to Technical Standards is requested for more than 5 sets, the applicant will be asked to apply for type approval for the sets.
4) If the applicant is other than receiver of the shipment then he/she must provide authorization, for delivery of Certification of Compliance to Technical Standards. (Authority letter duly signed by the consignee is required).

Annex-1 to Appendix G-2

GOVERNMENT OF PAKISTAN

PAKISTAN TELECOMMUNICATION AUTHORITY

Address for issuing office i.e. HQ or Zonal office along with contact information

http://www.pta.gov.pkhttp://www.pta.gov.pk/

(Say No To Corruption)

Letter No9.499/2017/PTA Dated

Subject: Issuance of Certification of Compliance to Technical Standards

Reference: Your request dated _____ received on the subject.

PTA has no objection on release of below listed equipment imported under HAWB/parcel no_____ for personal use only.

Sr. No.	Model/Brand	Type	IMEI No.
1			
2			
3			
4			
5			

Note: Custom Authorities will perform physical verification of IMEI contained within the shipment, with the IMEI details reflected as part of this PTA issued Certification of Compliance to Technical Standards *prior to release of the shipment.*

2. PTA has no objection to re-export of devices to country of origin that are not included in the aforesaid table (equipment detail). Tablet PCs without SIM functionality are exempted from Certification of Compliance to Technical Standards/ Type Approval process, Custom may release as per their procedure.

4. In case of any query regarding this Certification of Compliance to Technical Standards, you may contact at following address/phone/fax /email:

Director General Services, PTA HQ's, F-5/1, Islamabad.
Phone: 051-9216767
Fax: 051-9215544
E-mail: typeapproval@pta.gov.pk

Zonal Director
(Khi/Lahore/Rawalpindi/Quetta/Peshawar)

To:

Deputy Collector Customs where shipment is detained

Cc:

1. **Applicant**
2. **Director Type Approval, PTA Headquarters**
3. **Director General Services, PTA Headquarters**

Appendix H

Revised SOP on Implementation of Blocking of Stolen/Snatched Mobile Phonesthrough IMEI Number

PTA had formulated a comprehensive SOP to block SIMs in case mobile phones get snatched. The SOP remained implemented for Karachi City in phase-I from the year 2004. The same was planned to be extended to other parts of the country (major cities) in phase-II. However, with a view to make the methodology more effective, possibility of blocking Mobile Phone was explored and deliberated instead of blocking SIMs which did not produce desired results.

As a consequence of in-depth deliberation and discussion sessions held with stakeholders, government functionaries and vendors, all possible options including establishment of CEIR were analyzed. Consensus was to keep the implementation process as simple as possible so that it yields maximum results without incurring heavy cost, for which the stakeholders were also not convinced.

After having consensus of all the stakeholders for a way forward, PTA is formulating revised version of the current SOP to include the blocking of **Cell Phones** through IMEI numbers instead of blocking **SIMs.** To be able to combat the situation, it has been decided to implement the SOP/Policy in letter & spirit for which **following measures needs to be taken as "Step I" for effective implementation:**

a. All CMTOs will install EIR facility in their switches and make it operational before September 2006 for blocking the mobile phones all over the country. Options of creating CEIR in the country will not be pursued to keep the implementation of the policy simpler and cost effective.

b. CPLC Karachi will continue to provide IMEI numbers required to be blocked/unblocked as per the procedure already being practiced till implementation of revised SOP of blocking cell phones.

c. Country wide registration of complaints as per the regulations will be initiated after sorting out modalities with Provincial/Local Law Enforcement Agencies (LEAs) for making the **policy of data base sharing effective at national level.** Data base for **black list mobile sets** only be maintained at **three locations** i.e CPLC/Designated Police, CMTOs and Association of the Dealers (dealing in old mobile sets).

d. CMTOs may link/synchronize their data with Centralized EIR maintained at Dublin Ireland for enhanced requirements.

e. Unified Format for making such complaints attached as **Annex A** to this Appendix**.** Complaint must be registered with concerned Mobile Operator, CPLC/Police and Dealers Association with in 24 hours.

Responsibilities/Actions of the Stakeholders shall be as under:

1. Provincial Government

The Provincial Government will educate the public on how to prevent their mobile phones from being stolen and what to do in case the phone gets stolen. Mobile phone set holders will also be educated how to retrieve and record IMEI (International Mobile Equipment Identity) number (i.e. by feeding *#06#) of their mobile sets as being done by CPLC Karachi currently. Details are:

a. CPLC/Designated Police will obtain the information regarding stolen mobile sets from various sources (like individual complaints, Police Helpline 15, etc.) and inform all CMTOs giving the IMEI numbers and related details for entering the stolen IMEI numbers on their GSM network for blocking stolen/snatched mobile phones.

b. CPLC/Designated Police will record the IMEI numbers of stolen phones and will share the information with Law Enforcing Agencies and members of Electronic Dealer Association of a particular city/area (like being done by Karachi Electronic Dealers Association) who deals in the second hand mobile phone sets.

CPLC/Designated Police will be responsible for authenticity of complaints. CMTOs will block/unblock only after written instructions/clearance from CPLC/Designated Police.

2. Police Helpline 15

Police Helpline 15 will register the complaint, record it, and give case number to the complainant while ensuring his credentials. Police Helpline 15 will provide the data of all the recorded complaints to CPLC-5682222/Designated Police to store it in the data base.

3. Subscriber of Mobile Phones

In case of theft, the subscriber will inform police helpline 15/CPLC-5682222/Designated Police for the purpose to register his complaint, giving IMEI number and his own credentials. He will obtain the case number of his complaint from police helpline 15/CPLC-5682222/Designated Police. CPLC/Designated Police to develop software to maintain the record of stolen/snatched mobile phones.

4. Cellular Mobile Companies

a. The cellular mobile companies on receiving the IMEI numbers of stolen phone sets will enter them on their GSM network and block the cell phone sets.

CMTOs will block or unblock mobile phones only on receiving written instructions from CPLC/Designated Police.

b. Before blocking, concerned mobile company will send an SMS to the subscriber informing him that he is using a stolen/snatched mobile phone set for which he needs to clarify his position, to save himself from legal consequences/embarrassment. The format of SMS will be:

"Dear Customer! You are using stolen/snatched phone. Your cell phone set is being blocked. Contact CPLC-5682222/Designated Police for information/clearance".

c. The cellular mobile companies will also educate their subscribers, how to retrieve and record the IMEI number of their mobile sets through SMS/media (by feeding *#06#).

d. Each CMTO will designate an officer for these purposes at all major cities for coordination/liaison with CPLC/Designated Police. They will intimate his name, designation, address and contact numbers to CPLC/Designated Police under intimation to PTA within 10 days of issuance of this policy. CPLC/Designated Police and PTA will be updated in case the designated officer is changed.

e. "Awareness Drive" through electronic and print media will be launched by all CMTOs making the general public familiar with IMEI number and its retrieval/recording procedure, for at least three months.

6. Mobile Phone Set Dealers

a. The dealers, after receiving the information about stolen phone sets, will also prepare the database for stolen mobile phone IMEI number to prevent purchase/sale of these sets.

b. They will also inform LEAs and CPLC/Designated Police in case stolen mobile sets are detected at the time of sale purchase of the mobile sets.

7. PTA

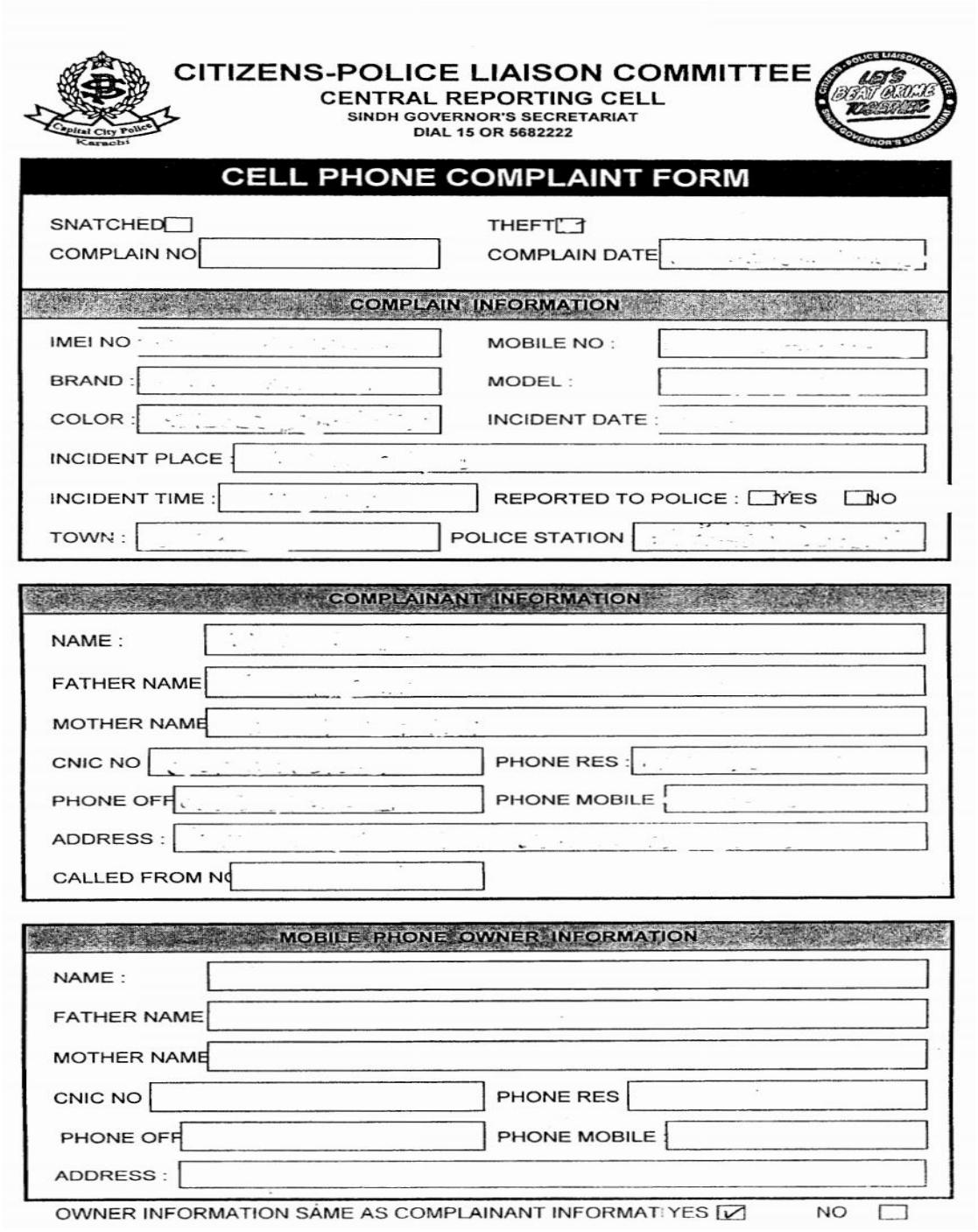
a. PTA will instruct and ensure that all mobile companies cooperate with CPLC/Designated Police and enter the IMEI number of stolen phone sets on their GSM network and block their operation.

b. PTA Zonal Office will render every possible assistance/technical support, if required, to the Provincial Government.

8. Ministry of Interior (Moll

Mol will approach Law Ministry to formulate and incorporate appropriate law/rule which declares tempering of IMEI number and or assisting in tempering as a serious crime/offence punishable with two years imprisonment along with penalty of fine.

Annex A to Appendix H



CITIZENS-POLICE LIAISON COMMITTEE
CENTRAL REPORTING CELL
SINDH GOVERNOR'S SECRETARIAT
DIAL 15 OR 5682222

CELL PHONE COMPLAINT FORM

SNATCHED ☐ THEFT ☐
COMPLAIN NO _____ COMPLAIN DATE _____

COMPLAIN INFORMATION

IMEI NO _____ MOBILE NO : _____
BRAND : _____ MODEL : _____
COLOR : _____ INCIDENT DATE : _____
INCIDENT PLACE : _____
INCIDENT TIME : _____ REPORTED TO POLICE : ☐ YES ☐ NO
TOWN : _____ POLICE STATION : _____

COMPLAINANT INFORMATION

NAME : _____
FATHER NAME _____
MOTHER NAME _____
CNIC NO _____ PHONE RES : _____
PHONE OFF _____ PHONE MOBILE _____
ADDRESS : _____
CALLED FROM NO _____

MOBILE PHONE OWNER INFORMATION

NAME : _____
FATHER NAME _____
MOTHER NAME _____
CNIC NO _____ PHONE RES _____
PHONE OFF _____ PHONE MOBILE _____
ADDRESS : _____

OWNER INFORMATION SAME AS COMPLAINANT INFORMAT: YES ☑ NO ☐

Annex-B
To Enf Div letter No.17-22/2012/Enf/PTA
Dated:September, 2012

STANDING OPERATING PROCEDURE (SOP)

BLOCKING MOBILE NUMBERS/IMEIS INVOLVED IN KIDNAPPING FOR RANSOM AND IN EXTORTIONS CASES

INTRODUCTION

1. An Authority Level meeting was held on 30th August, 2012 to discuss the issue of unverified SIMs. The meeting was attended by MoIT, Cellular Mobile Operators, CPLC representatives and chaired by the Chairman. During the meeting Chief of Citizen Police Liaison Committee (CPLC) requested the Authority to help out in eradication of kidnapping for ransom and extortions crimes through blocking of SIMs and IMEIs of the individual involved, which was done earlier by PTA. In order to help the citizens of Karachi in such difficult time, the Authority has agreed to the proposal of Chief CPLC for blocking of SIMs/IMEIs in kidnapping of ransom and extortion cases.

HANDLING OF INFORMATION BY STAKEHOLDERS

2. Only one point of contact from CPLC and mobile operators will be authorized to handle such cases. Chief CPLC and mobile companies will intimate the name, appointment, telephone numbers (landline and mobile), fax and email of the focal persons to PTA Karachi Zone.

REQUEST PROCESSING PROCEDURE

3. Following procedure shall be adopted to streamline the whole process:-

a. CPLC RESPONSIBILITIES

- CPLC shall ensure submission of only genuine complaints. In case of bogus / fake complaint, the liability shall be on CPLC and PTA will bear no responsibility.
- The designated person of CPLC shall make a request of blocking of SIM/IMEI to PTA Karachi Zone in writing on CPLC letter head.
- The request from CPLC shall enclose attested copies of following documents: - o Copy of Complaint
  o CNIC of complainant
  o FIR (If applicable) o

Any other related information

- The designated person of CPLC shall coordinate with following Officers of PTA Zonal Office Karachi in case of any difficulty: -

Deputy Director (Enforcement) (Principal) PTA Zonal Office, Wireless Compound, Opp: JPMC, Rafiqui Shaheed Road, Karachi-75530, Phone #: 021- 35211285, Fax #: 021-5680640 Assistant Director (Enforcement) (in absence of Dy. Director) Address: PTA Zonal Office, Wireless Compound, Opp: JPMC, Rafiqui Shaheed Road, Karachi-75530, Phone #: 021- 35680137 ,Fax #: 021- 5680640

b. PTA KARACHI ZONE'S RESPONSIBILITIES

- It shall be ensured that all such requests are handled as quickly as possible but not later than two (2) hours.
- On receiving a complaint alongwith all relevant documents, PTA Karachi Zone will direct the designated persons of the operators for immediate blocking of the SIM/IMEIs.
- Zone shall confirm the blocking of SIMs/ IMEIs to CPLC after receipt of the same from mobile operators.
- Zone shall submit monthly summary of all blocked SIMs/ IMEIs of such complaints to Enforcement Division PTA HQs for the information of the Authority, on or before 5th of every month as per following format: -

S. #.	CPLC				PTA KARACHI ZONE		Remarks
	Letter No.	Date	SIM#	IMEI #	Blocking Date	Operators Confirmation	

c. MOBILE OPERATORS RESPONSIBILITES

- Designated focal person of Mobile Operators will block the SIMs/IMEIs within two (2) hours of the receipt of the request from PTA Karachi Zone.
- After blocking of the SIMs/IMEIs, the same shall be confirmed to PTA Karachi Zone through return email.

Conclusion

3. This SOP is devised only to help CPLC in Karachi City and will have no legal binding on PTA. The SOP may be amended from time to time as and when required.