I/3043360/2022

Restricted

F. No. 37-4/2021-DGTHQ/3
Department of Telecommunications
Ministry of Communications
(DGT HQ)

UIDAI Building, Bangla Sahib Road
New Delhi-01, Dated .05.2022

Subject: Standard Operating Procedures (SOP) for checking Grey Market Operations - regarding

This is in reference to SPPI wing letter no. 19-62/2019/S-II (E-93013) dated 18.05.2022 regarding subject cited above where in SOP for checking grey market operations has been enclosed.

2. It is intimated that the SOP/algorithms should be implemented immediately with a target to achieve results within next 30 days.

4. The SOP issued vide DoT letter no. 19-62/2019/S-II (E-93013) dated 18.05.2022 will be in supersession of this office instructions issued vide letter no. 37-4/2021-DGTHQ/3 dated 20.10.2021 (copy enclosed).

5. In view of above, LSAs are instructed for immediate implementation of the SOP issued vide DoT letter 9-62/2019/S-II (E-93013) dated 18.05.2022 (copy enclosed).

Signed by Aman Chawla
Date: 25-05-2022 11:32:32
Reason: Approved

Enclosed: As above

(Aman Chawla)
ADG-2 (Security & Rural)
Email – adgs2.hq-dgt-dot@gov.in
Tel: 011 23746145

To,

All LSA heads

Restricted

No. 19-62/2019/S-II (E-93013)
Department of Telecommunications
(SPPI wing)

Dated 18.05.2022

Subject: Standard Operating Procedures (SOP) for checking Grey Market Operations-Reg

A Committee was constituted for drafting and finalization of SOP for checking Grey Market Operations, vide DoT letter no. No. 19-62/2019/S-II dated 16th March 2022. The committee has submitted its report on 06.05.2022 and finalized the SOP. The copy of the approved SOP is enclosed herewith.

2. The Committee has recommended phased implementation of SOP for ensuring compliance and necessary action by LSA field units and TSPs/ISPs.

SoP implementation may be driven by the phased implementation i.e.

Phase-1: Portal based workflow for Call Center & suspected cases received from TSPs and its lifecycle management before DIU implementation and

Phase-2: On implementation of DIU, merging of phase-I workflow with suggested workflow in SIM box Analytics and Prevention System (SAPS) module of DIU.

AS Wing has been requested to examine and incorporate the suggested workflow while preparing the architecture and functional requirements of SAPS module in DIU system.

3. In this regard, it is requested that necessary action may be taken with regard to SOP for ensuring compliance/necessary action by LSA field units.

4. This issues with the approval of Secretary(T).

Encl. As above

18/5/22

(R S Singh)
Director (Security)
011-23036337

To,
The DGT
Sanchar Bhawan
New Delhi

Copy to:
1. DDG(AS),DoT, New Delhi

Standard Operating Prodedure(SOP) for handling Grey Market Operations

At present, suspected cases/inputs with respect to Grey Market Operations are being received from either DoT Call Centre or TSPs. Currently, there is no integrated system and as such all the processes are working in off-line mode. However, once SIM box Analytics and Prevention System (SAPS) Module of DIU is operationalized, work flow management including CDR analysis of suspected cases/inputs received from DoT Call centre and TSPs would be integrated with the SAPS module of Digital Intelligence Unit (DIU) for effective analysis, tracking, enabling timely collaboration by LSAs/TSPs/ISPs, and thereby making the entire process online. Based on above facts, the following SoP should be adopted by LSAs for detecting and handling the cases of suspected grey market operations in various scenarios:

A. Complaints received in DoT Call Centre:

a. Complaints received in DoT Call Centre are forwarded to concerned LSA on the basis of received CLI or MSISDN of the Complainant / Informer (called number).

b. To verify the veracity of complaint / information, CDR of the MSISDN number of the Complainant / Informer is analysed by concerned LSA.

c. If the reported number (calling number / 'A' number) appears in the CDR, then the case is forwarded to the concerned LSA otherwise the case may be closed.

d. LSA, to which the reported number (calling number / 'A' number) belongs to, shall obtain CDR of the number for the past one month, after ascertaining the identity of the subscriber. If the number is roaming in some other LSA, then the case may be forwarded to that LSA with all details. However preliminary analysis needs to be done by LSA to which the number belongs.

e. **If the suspected number ('A' number) is a mobile number :**

(i) The CDR is analysed w.r.t. outgoing calls, distinct number percentage, IMEI of SIMBOX, different Cell IDs, etc. Some of the called numbers from the CDR can be manually called by LSA officials to confirm as to whether the call received is domestic or international.

1. If most of the holders of called numbers report that the incoming call was international then the 'A' number is suspected to be part of a grey market setup.

2. If the calling pattern is normal, the case may be closed.

(ii) In case the 'A' number is suspected to be part of a grey market set-up, then CDR of all IMEIs with the same TAC code as that of suspected IMEI in that location or CDR for the BTS IDs may be obtained, to get other MSISDNs used by the setup.

f. **If the suspected 'A' number is of SIP lines/PRI lines,** CDR is analysed w.r.t. outgoing calls, incoming calls, distinct number percentage etc. Some of the holders of called numbers from the CDR can be called manually to confirm as to whether the call received was domestic or international.

    1. If most of the holders of called numbers report that the incoming call was international then the 'A' number is suspected to be part of a grey market setup.

    2. If the calling pattern is normal, the case may be closed.

g. Complete case (in both categories, whether Mobile or SIP/PRI lines) shall be forwarded to LEAs for further analysis with all the details like CDR, all MSISDNs found out, customer details, details of call made by LSA etc (by home LSA or LSA in whose jurisdiction the illegal setup is located).
h. Further LSA shall actively co-ordinate with LEAs to unearth the setup.
i. After identification of location by LEA/LSA, LSA has to ensure that TSPs/ISPs shall lodge complaint with LEA for conducting raid within 48 hours
j. Details of resources found in the setup and data like CAF, CDR, IPDR etc are to be provided by TSP/ISPs within 48 hours to LEAs / LSAs

k. There should be no disconnection of resources by TSPs/ISPs without the consent of LSA

l. Representatives of TSPs/ISPs who are present at the raid spot shall sign the inspection report / network diagram of the telecom setup / certificate regarding the usage of the telecom setup etc.

m. Joint raid report be prepared and signed by all concerned present during the raid.
n. FIR would invariably be filed by LEAs/State Police based on inputs/reports provided by TSPs/LSA.
o. Above processes/workflow should be made portal based.

B. Suspected numbers received from TSPs :

(a) Fraud Management System (FMS) deployed by TSPs may use following set for parameters/rules and their combination to identify suspected numbers:

    i. Cumulative OG call duration : More than 120 minutes per day

ii. % Outgoing calls: More than 90% OG calls
iii. % Incoming calls : Less than 5%
iv. Cumulative IC call duration : Less than 30 minutes per day
v. % distinct numbers called: More than 80 %
vi. No. of different cell IDs : Less than or equal to 3

The threshold given above is notional and indicative in nature. These set of parameters/rules should be dynamically configurable. DGT unit may review from time to time and fix the value of threshold based on the experience of field units and atleast once in a year.

TSPs shall report suspected number along with all their findings (parameters and observation from sample calling, test calling facility, etc) as analysed by their FMS to LSAs on regular basis.

After the operationalization of SAPS module of DIU, TSPs will upload the report of suspected mobile numbers as detected by their FMS System along with relevant details which includes data like CAF, CDR, IPDR etc in the SAPS Module directly.

(b) On receipt of list of suspected numbers from TSPs, the concerned LSA shall obtain the CDRs of these numbers for the past one month. If the number is roaming in some other LSA, then the case may be forwarded to that LSA with all details. However preliminary analysis needs to be done by LSA to which the number belongs.

From this step onwards, all steps as mentioned from Sl. No. (e) to Sl. No. (o) of para A above should be followed.

C. Suspected numbers identified by SAPS upcoming Module based on Data analytics and AI/ML algorithm through Digital Intelligence Unit (DIU)

It is envisaged that SAPS module would source all relevant data like SDR including that of ILL/PRI/SIP trunks etc., IMEI analysis from DIU-CEIR, feeds from TSPs, CDRs etc. A detailed analysis collating SDR, IMEI, IMSI and CDR data will be done to uncover suspicious/illegal telecom setup & SIM box activities.

After the operationalization of DIU, SAPS module after detailed data analytics based on AI/ML algorithm will also give alert for suspected numbers.

After gathering the machine intelligence from DIU, the inputs shall be analyzed in detail by the concerned LSA. In case, it is found that it is a suitable case of suspected clandestine / illegal telecom setup activity, appropriate measures are to be taken to unearth these setups as mentioned from Sl. No. (h) to Sl. No. (o) of para A above should be followed.

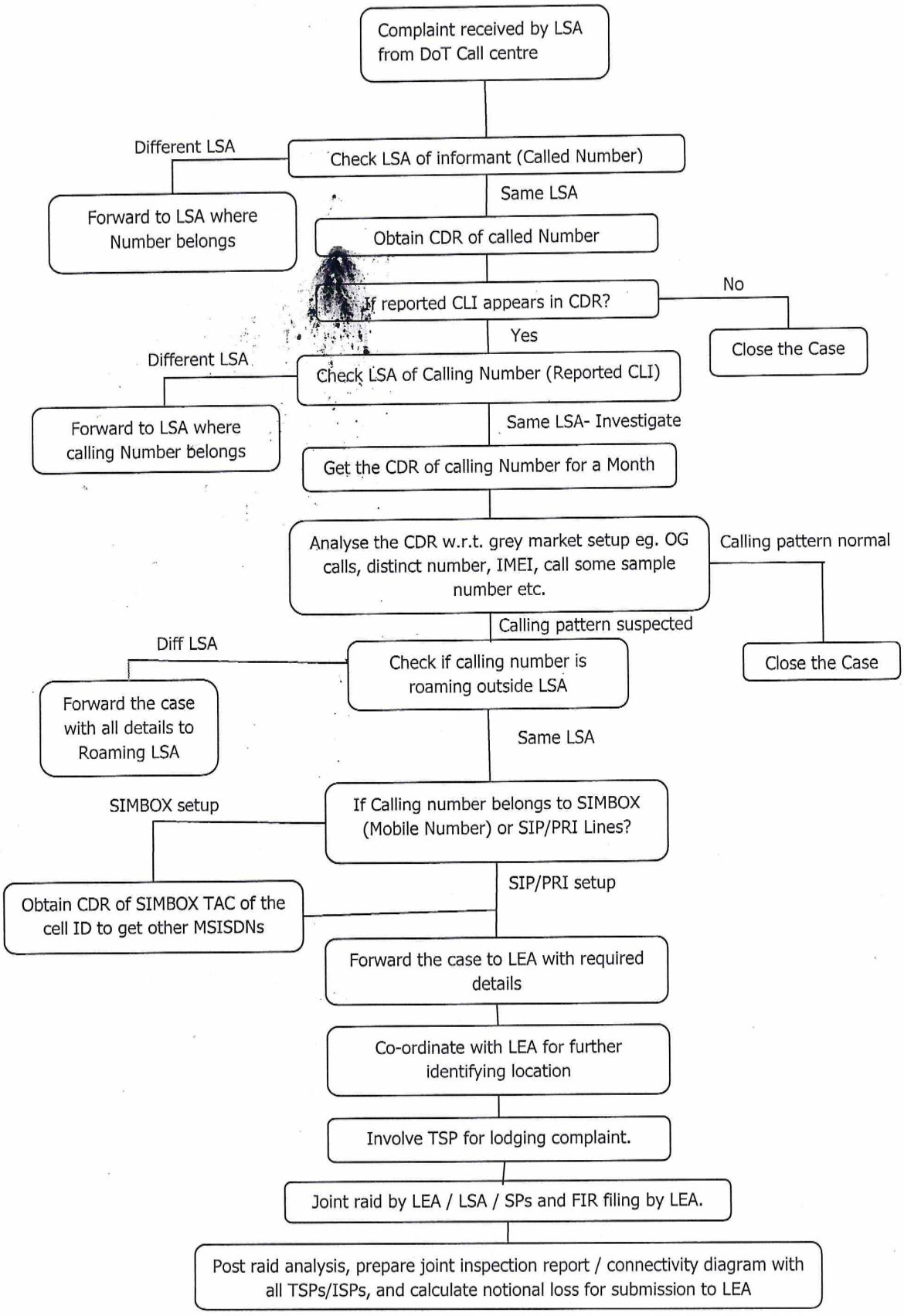


Fig-1-LSA Flow Chart for Complaint DoT Call Centre

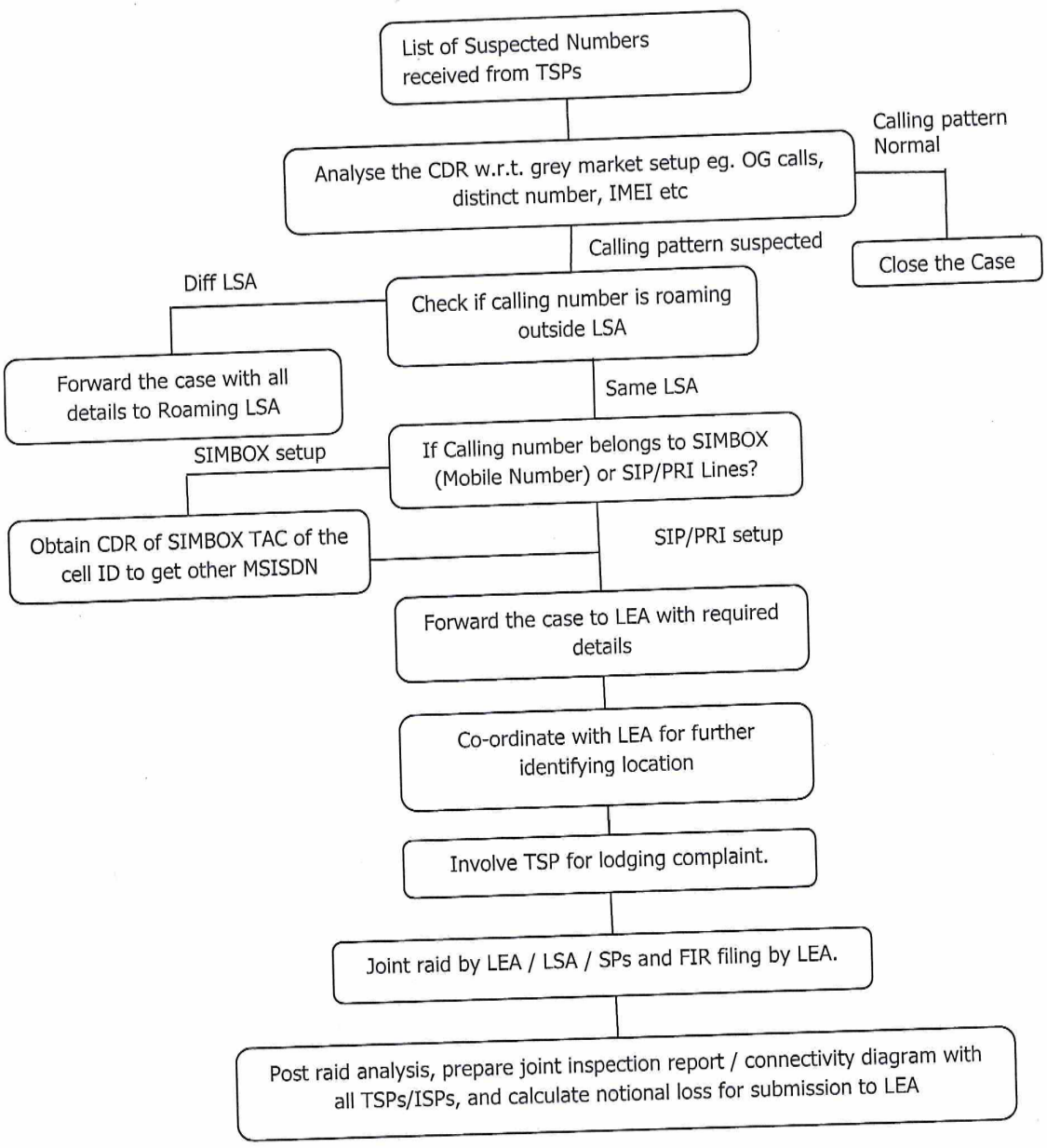


Fig-2-LSA Flow Chart for list of suspected numbers received from TSPs

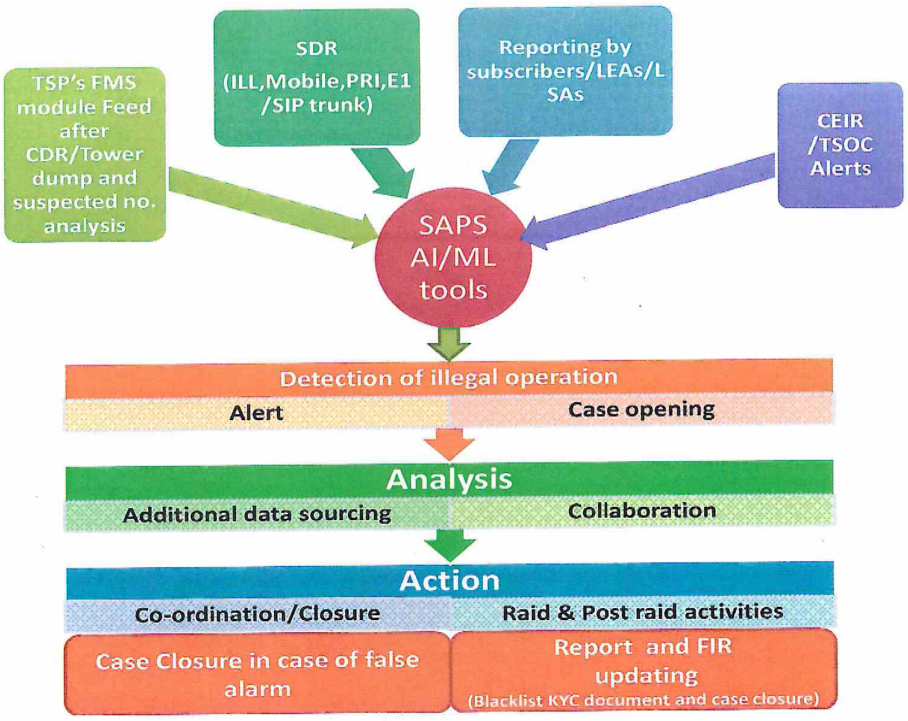


Figure-3- Indicative Workflow in SAPS Module of DIU

(D) Post-raid analysis by LSAs: Following post-raid activities may be undertaken by the LSAs.

I. **Arriving at Notional Loss**: CDR/usage pattern of seized SIM Cards, SIP trunk Nos. etc are analysed for loss calculation and to identify other such set-ups. There are two components involved while calculating the notional loss i.e. one loss incurred by **International Long Distance Operators** (ILDO) and two **by Access service providers**) which also result into loss incurred to exchequers (Govt. on India) in terms of License fee.

(a) Notional Loss Calculation for Telecom Service Providers

	Item	Formula	Remark
1	Total Out Going Minutes	A	calculated from CDR of telecom resources used by illegal setup
2	International Settlement Charges (ISC) per minute	B	Revenue of ILDO
3	International Termination Charges (ITC) per minute	C	Revenue of access service providers
4	Approx. Notional Loss to ILDO operator	D=A*(B-C)	
5	Approx. Notional Loss to access service providers	E=A*C	

6	Total approx notional loss to Indian Telecom operators (ILDO and access service providers)	F= D+E	

(b) Notional Loss Calculation for Department of Telecommunications, Government of India

	Item	Formula	Remark
1	License Fee @ 8% of Adjusted Gross Revenue (AGR) of Licensee : ILDO	G=D*0.08	
2	License Fee @ 8% of AGR of Licensee: access service providers.	H= E*0.08	
3	One time Entry Fee for obtaining ILD License	I	Rs 2,50,00,000/- (at present)
4	Processing Fee for obtaining ILD License	J	Rs 50,000/- (At present)
5	Total approx notional loss to DoT, Government of India.	K=G+H+I+J	

ISC: The revenue to the ILDOs in India for legal international incoming calls is in the form of the International Settlement Charges (ISC). Hence when such incoming calls are bypassed through the grey route, revenue to the ILDOs involved for each such calls are lost. It was not possible to ascertain source country of these international calls and different countries charge different ISCs. As such, for this purpose average ISC collected by major ILDOs shall be taken as ISC. This figure shall be released by DGT after obtaining from major ILDOs on quarterly basis to all LSAs for calculation of loss.

ITC: There is Revenue loss to the access service providers (domestic TSPs) as well in the form of losing out on International Termination Charges (ITC) earnings. The ITC has been revised to Rs. 0.35 – Rs. 0.65 / minute w.e.f. 01.05.2020. (Please refer TRAIs, The Telecommunication Interconnection Usage Charges (Sixteenth Amendment) Regulations, 2020 Dated 17.04.2020 and The Telecommunication Interconnection Usage Charges (Fourteenth Amendment) Regulations, 2018 Dated 12.01.2018). The maximum recommended and latest ITC shall be taken as ITC for calculation of loss in above formula.

II. Analysis of IPDR of internet connection used in the illegal setup may be done. It may be possible to get the IP address of the SIP server / proxy server / remote server / DDNS server which were accessed by the SIM box. All ISPs may be asked about the customers who accessed these remote IP addresses from India. The subscriber accessing these remote IP addresses might be possible SIM box setups.

III. SDR/CAF for the telecom resources used in set-up like SIMs, SIP Trunks, ILL lines etc. may be obtained to check if they are provisioned as per extant rules/orders/guidelines. CAF audit is to be carried out to verify the bonafide of the subscriber and accordingly, penalty may be imposed on TSPs/ISPs in case of CAF non-compliance as per license conditions/guidelines. POS/retailers of specific city / location, who may be an accomplice in the crime may be identified and their role be investigated accordingly. In this regard, LSA shall ensure that TSPs file a proper complaint with LEAs against the errant PoS / customers within one week of the raid.

IV. LSA shall ensure the disconnection of resources used in raided location by TSPs.

V. A black list of KYC documents used in getting telecom resource may be maintained which may be updated in DIU module as soon as it is implemented so that such KYC documents may be red flagged at the time of new telecom service subscription. The process of KYC undertaken by TSPs may also be reviewed for such detected case.

VI. Post-raid activities may preferably be completed within a month of the raid.

(E) Suggested Additional points for early detection and check grey market Operation

(i) A mechanism of monthly co-ordination meeting between LSA officials and State Police / State IB may be established at each LSA for intelligence gathering and preparing strategy for conducting raids.

(ii) To encourage more reporting of illegal CLIs by Public, wide publicity may be given through public platforms. Some additional channels of reporting like SMS Social Media platforms etc. may also be added.

(iii) Monthly review of status of detected cases through Call Centre/TSP/SAPS detected cases may be done and reported to DGT unit for ensuring timely action.

(iv) Ensuring Routine Inspection of IPLC/ILL/PRI/SIP Customers by LSAs as per DoT Guidelines.

***

I/3033390/2021

F. No. 37-4/2021-DGTHQ/3
Department of Telecommunications
Ministry of Communications
(DGT HQ)

Sanchar Bhawan, 20, Ashoka Road
New Delhi-01, Dated .10.2021

Subject: Instructions to LSA field units to undertake the exercise for detection of clandestine telecom setups on regular basis **-** reg

In view of frequent instances of unearthing clandestine exchanges reported from various parts of the country, this office was requested to issue detailed instructions to LSA field units to undertake the exercise for detection of clandestine telecom setups on regular basis.

2. In this regard, the LSAs are requested to undertake the exercise for detection of clandestine telecom setups on regular basis. While doing the exercise, the LSAs may carry out various activities including but not limited to mentioned in Annexure –I (copy enclosed) as per the guidelines issued by DoT in the subject matter from time to time.

This is issued with the approval of competent authority.

Encl: As above

Signed by Aman Chawla
Date: 20-10-2021 15:11:58
Reason: Approved

(Aman Chawla)
ADET-1 (Security & East)
Email: adets.hq-dgt-dot@gov.in
Tel: 011-23746145

To,

All LSA Heads

Annexure-I

Activities to undertake the exercise for detection of Clandestine Telecom Setups on Regular basis

1. **Analysis of inputs received from DoT Call Centre** (1800110420 or 1963) in Rajasthan LSA. The detailed procedure is attached as **Annexure-II.**
2. **CDR analysis to be done by TSPs/LSAs**: The CDRs of the numbers may be checked to ascertain any usage of telecom resources in organised fraudulent activities by following the algorithm (LSAs can improvise below given algorithm to achieve the objective)
   i. The numbers are static numbers i.e. not making use of more than Three BTS
   ii. The calling pattern is highly asymmetric i.e. more than 95% calls are outgoing
   iii. The called numbers are random numbers not getting repeated in a span of seven days i.e. degree of distinctness is more than 80% in seven days
   iv. The numbers are being recharged from the same MSISDN/person/POS/Retailer

   This will enable in identifying the criminal hotspots and emerging criminal hotspots.

3. **Traffic data (Internet / BTS traffic) analysis by TSPs/LSAs**–Internet subscribers with equal upload & download volume may be identified (MRTG) as it may be part of an illegal telecom set up. The inspections can be carried out at such subscribers' premises. Further BTS traffic data may be analysed. High % of outbound calls from any specific BTS may be because of presence of illegal setups in the area.

4. **SIP Trunk Pattern Analysis**: LSA should direct TSPs to analyse the calling pattern of SIP trunk (all numbers including pilot number) using their FMS (fraud management system) and list of SIP trunk customers with vital details (technical as well as non-technical) to be submitted to LSA concerned on monthly basis.

5. **Identification of POS operating from outside LSA boundary:** Most of the SIM cards used in grey market are sold through fraud manner on fraud Identity. LSAs can identify such fraud number by extracting Lat-long of POS mobile from subscriber database and can be seen if any POS is selling SIM card outside the boundary of LSA.
6. Action on Individual bulk connections identified by **TAFCOP**.
7. **Activities post identification of Illegal setup/ Post Raid Analysis:**
   i). Analyse the CDR/usage pattern of seized SIM Cards, SIP trunk Nos. etc
   ii). Find out specific POS/Retailers and POS/retailers of specific city / location, who may be an accomplice in the crime and the role of POS/Retailers is investigated.
   iii). Find out whether numbers are being recharged from same PoS/Retailer
   iv). Find out whether SIMs are in home LSA or Roaming.
   v). Obtain SDR/CAF for the seized SIMs, SIP Trunks etc.
   vi). Find out whether a telecom resources viz. SIMs/Internet connections etc. were provisioned as per extant rules/orders/guidelines. CAF audit and connection

verification for CAF compliant numbers is be carried out to verify the bonafide of the subscriber and accordingly, appropriate action is taken on TSPs/ISPs in case of non-compliance.

vii). Disconnection of suspected telecom resources i.e. connection (SIM/Internet/PSTN) blocking, IMSI Blocking, Internet SIP trunks etc.

8. **Awareness Program by LSAs/TSPs**: LSAs in coordination with TSPs shall launch awareness campaign among the citizens regarding the
   i. Nation Cyber Crime Reporting Portal operated by I4C unit of MHA to lodge cybercrime complaints and
   ii. DoT Call Centre to lodge Grey Market complaints.

Annexure-II

General Process to be followed by LSAs for cases received from DoT Call Centre:

If 'A' is the recipient of International call from local Number 'B'

Step 1: Find TSP and LSA to which MSISDN's A & B belong to - From MNPO Service Provider Platform
Step 2: Transfer the case to other LSA - If MSISDN A belongs to other LSA
Step 3: Further Investigate the case - If MSISDN A belong to same LSA
Step 4: Obtain CDR of A - Verify the said call event in CDR i.e whether Party A actually received a call from Party B

i. Further investigate the case - If positively verified
ii. Close the case If Negatively Verified
iii. (Transfer the case to other LSA with investigation summary & also highlight the said call event in CDR - If MSISDN B belongs to other LSA

Step 5: Obtain subscriber details of MSISDN B if B belongs to same LSA Ascertain the identity of the subscriber
Step 6: Obtain CDR of past 1 year for Party B

i. Check for suspected calling pattern
ii. Close the case - calling pattern of B is "Normal/Non- Suspect"
iii. Further investigate - calling pattern is verified to be suspected

Step 7: From CDR of B: -

i. Find out whether IMEI/s belong to SIM Box (from GSMA Portal)
ii. Find out details of BTS such as BTS Id, BTS Location, BTS Address etc to which the suspected MSISDN B gets latched

Step 8: Obtain LBS/Location/Coordinates of the Suspect Party B
Step 9: Obtain details of all Internet Users with "Nearly Equal Upstream and Downstream Volume" in the area near to LBS/Location/Coordinates of suspect party B - As per ISP License Clause 34.15 (It is observed that illegal telecom set ups utilize Internet with nearly equal Upstream and Downstream volume).

Step 10: Analyse Tower Dump of BTS/BTS's to which Party B gets latched to - Find out all other IMEI's and MSISDN's that are suspected to be part of illegal activity.
Step 11: Recce of suspected premises with the help of local police**:** Correlate all the intelligence gathered in above steps & exactly locate illegal telecom set up.
Step 12: Once the illegal setup is detected by DoT (LSAs) or LEAs, the TSPs/ISPs are intimated to extend unconditional support to DoT/LEA at the raid location; depute their representative/s at raid location and also lodge FIR. Contact details and Escalation matrix must be clearly intimated by the licensee to DoT in order to avoid any sort of delay during raid activity
Step 13: Finally, details must be submitted these to the LEA for further investigation & busting.