F.No.H-19011/2/(Misc)/2019-CDN/CFN3464487

Government of India
Ministry of Home Affairs
Police Modernization Division
Provisioning Desk

26 Man Singh Road,
Jaisalmer House, New Delhi.
Dated the 29th October, 2020.

OFFICE MEMORANDUM

Subject: Standard Operating Procedure (SOP) to address security concerns while procuring Radio Communication equipment.

The undersigned is directed to say that in order to ensure secure radio communication, an SOP has been formulated by this Ministry. (Copy enclosed)

2. Henceforth, all CAPFs/CPOs shall ensure that the SOP is duly followed.

3. This has the approval of the competent authority.

Enclosure: As above.

(Achyut Singh)
Second –In-Command (Provisioning), MHA
Tel: 233836034

1. DsG/Director: AR, BSF, CISF, CRPF, ITBP, NSG, SSB, NCB, IB & NIA.
2. Commissioner of Police Delhi, 2nd Floor, Tower I, Delhi Police Headquarters, Jai Singh Road, New Delhi.
3. Director DCPW, Block No. 9, CGO Complex, Pragati Vihar, New Delhi-110003.

SOP to address security concerns while procurement of Radio Communication equipment

1. Preference may be given to the Radios manufacturers in India, as the corresponding OEMs would be more likely to be co-operative in meeting the requirements of Testing Agency as well as meet the specified security and trustworthiness requirements completely and correctly.

2. Following suitable mandatory clause may be incorporated in the tender/bid document while floating the tender/bid for procurement of equipment for radio communication.

A. Malicious Code Certificate:

The seller should upload following certificate in the bid:-

(a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:-

i. Inhibit the desired and designed function of the equipment.

ii. Cause physical damage to the user or equipment during the exploitation.

iii. Tap information resident or transient in the equipment/network.

(b) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

Cont'd... P/2

159

B. As and when asked for, the firm shall share the complete Hardware (including disclosure of sourcing of critical components) / Software / Firmware details of the radio communication equipment with the procurement agencies/testing agencies.

C. The firm shall cooperate with the testing agency, as designated by the procurement agencies, to provide any further details/assistance, as and when sought by them.

D. If the Radio equipment supplied by the firm fails test by Testing Agency, the Bank Guarantee of the firm shall be invoked and suitable legal action shall be initiated against the firm

E. The firm will be blacklisted if it breaches any of the above mentioned clauses.

3. At any stage, in case of any security concerns with the Radio Equipment, the procurement agencies may contact the Testing Agency with complete details and direct the firm to provide details sought by the Testing agency and cooperate with them.

4. As abundant caution, all CAPFs to conduct annual security audit of their communication equipments.

***