

Tele Mil: 5915

BY ASIGMA

Military College of
Telecommunication Engineering
PIN – 908 768
c/o 56 APO

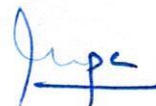
6621/AI Proj Whitelisting/GS (Tech)

23 Feb 24

**DDG IT, DGIS
IHQ of MoD (Army)
New Delhi 110010**

WHITELISTING OF AI BASED APPLS

1. Further to our letter No 6621/AI Proj Whitelisting/GS (Tech) dt 10 Feb 24.
2. In addn to the AI based appls, submitted for whitelisting vide our letter under ref, another AI based Pro-active Mobile Security Sys (PMSS) appl is submitted herewith for whitelisting. PMSS is a complete soln for malware scanning and banned appl detection that can be easily dply at Fmn HQ/ Units to monitor health of smartphones. The appl has been proliferated and dply in more than 36 locs pan IA.
3. The appl for whitelisting of PMSS as per format duly countersigned by Dy Comd & Chief Instructor, MCTE is encl as **Appx**.
4. For info and necessary action pl.



**(Anupam Sharma)
Lt Col
GSO-1 (Tech) B
for Comdt**

Encls :- (As above)

Copy to:-

ADB, HQ ARTRAC (IT Sec, GS Sec, Tech & Futuristics Sec), DG Sigs (Sigs 1, Sigs 7), CIDSS

SOC FOR WHITELISTING OF AI BASED PROACTIVE MOBILE SECURITY SYS (PMSS)**INTRODUCTION**

1. PMSS is a complete solution packaging malware scanning and banned app detection using Artificial Intelligence. It is an AI powered malware scanning station for smartphone/PCs devp in-house which is capb of detecting malware infection in a smartphone or PC without installing any agent or any physical contv with the scanning stn. The scanner uses latest state-of-the-art AI & Deep Learning algorithms for malicious traffic detection engine and a signature-based detection engine to supplement it. The scanner is capb of detecting the presence of malicious/banned apps merely by recording and analysing the network activity generated by the smartphone/PC being scanned. The scanning and analysis process only takes 3-4 mins per device.
2. PMSS is an extremely portable and low-cost malware scanning station which can be dply easily at fmn HQs / Unit As for periodic scanning and health check of smartphones/PCs. The scanner is very easy to use and designed with an intuitive UI. To use the scanner indls need to scan a QR code with their smartphones. The scanner then est a WiFi connection with the smartphone and analyses its network traffic using the onboard AI engine as well the Signature based engine. Thereafter, on board analytics is used to determine if the device has been compromised by malware or unwanted/banned apps have been installed. The scanner auto generates a detailed report which is shared with the user.

AIM

3. To devp an AI based portable proactive mobile security sys (PMSS) for malware scanning, banned app & contacts detection sys for impl in the units / fmn of IA.

OBJECTIVES

4. The AI based proactive mobile security sys will have the following objectives and features:-
 - (a) Indigenously conceptualised and in-house devp AI based soln mounted on an edge device making it portable and cost-effective appln.
 - (b) User-friendly GUI with the option of connecting smart device both through sys generated QR code and through physical connection using data cable.
 - (c) Device agnostic, agentless and non-invasive malware scanner.
 - (d) The cyber security package can be used to scan the smartphones of vendors, civilians emp in units, source/informers to ascertain if their smartphones are being used to spy on IA pers.
 - (e) Dply at entry/exit pts of Grn, Ord depots, office premises, comn centres, CSD depots etc for periodic scanning and checking of smartphones of pers moving in/out.

Annex I

(Ref Para 9 (a) of DDGIT letter
No B/04001/Policy/SW DDGIT
(T&P) dt 20 May 2020)

AI BASED PROACTIVE MOBILE SECURITY SYS (PMSS)

1. **Short Brief.** PMSS combines cutting-edge AI and Deep Learning algorithms along with a signature-based detection engine to detect malicious network traffic emerging/converging from/to a smart device. It identifies malicious applications by analysing network activity from the scanned smart device. The scanning process takes only 3-4 minutes per device, producing real-time reports in three categories. Additionally, the app enhances the cyber security by identifying and allowing one-click detection and removal of any banned applications on the smart device, thereby streamlining the cyber security assessment.

2. **Functional Purpose.** It is an AI powered malware scanning station for smartphone/PCs devp in-house which is capable of detecting malware infection in a smartphone or PC without installing any agent or any physical contact with the scanning station. The scanner uses latest state-of-the-art AI & Deep Learning algorithms for malicious traffic detection engine and a signature-based detection engine to supplement it. The scanner is capable of detecting the presence of malicious/banned apps merely by recording and analysing the network activity generated by the smartphone/PC being scanned. The scanning and analysis process only takes 3-4 mins per device. It is an extremely portable and low-cost malware scanning station which can be deployed easily at field HQs / Unit As for periodic scanning and health check of smartphones/PCs. The scanner is very easy to use and designed with an intuitive UI. To use the scanner, individuals need to scan a QR code with their smartphones. The scanner then establishes a WiFi connection with the smartphone and analyses its network traffic using the onboard AI engine as well as the Signature based engine. Thereafter, on-board analytics is used to determine if the device has been compromised by malware or unwanted/banned apps have been installed. The scanner automatically generates a detailed report which is shared with the user.

3. Specific details wrt SW proposed to be devp.

(a)	SW ID / Name (Incl ver number)	-	PMSS
(b)	Est/ Sponsor (Comd) (incl details of PDMG)	-	MCTE, Mhow
(c)	Type of SW (Bespoke/ ERP/COTS/Customized)	-	Customized.
(d)	Purposed/Utility (incl beneficiaries and tgt users)	-	Mobile Security
(e)	Name of devp org/ vendor name and contact details	-	MCTE, Mhow
(f)	Is IPR held with sponsor.	-	Under Process
(g)	OS & Sys software reqmts.	-	Win 10,
(h)	Language/ Platform of SW devp & dply	-	Python.
(j)	Database reqmts (software, ver, ect)	-	Nil.
(k)	Technology dependencies (if any)	-	AI
(l)	Cost incl Annual Maint Contract	-	40,000 for portable ver (Raspbeery Pie, 10 inch display, 32 GB Memory Card)

(m) Architecture to dply
(Centralized / Federated /Hybrid/ etc.)

- Can be dply in all mode

(o) Details of Licensing (if any)

- No.

(p) HW/Server specifications (if any)

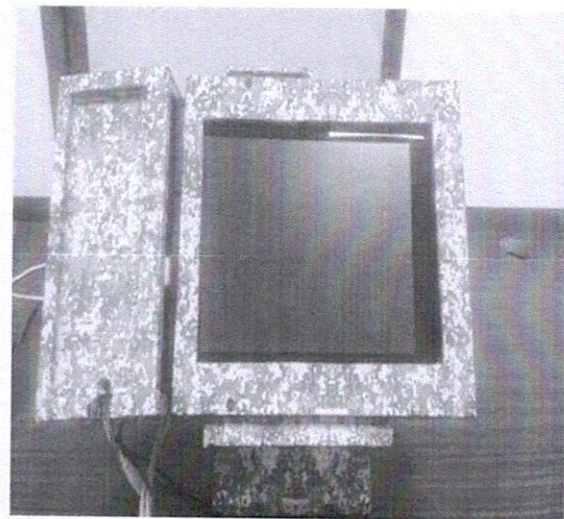
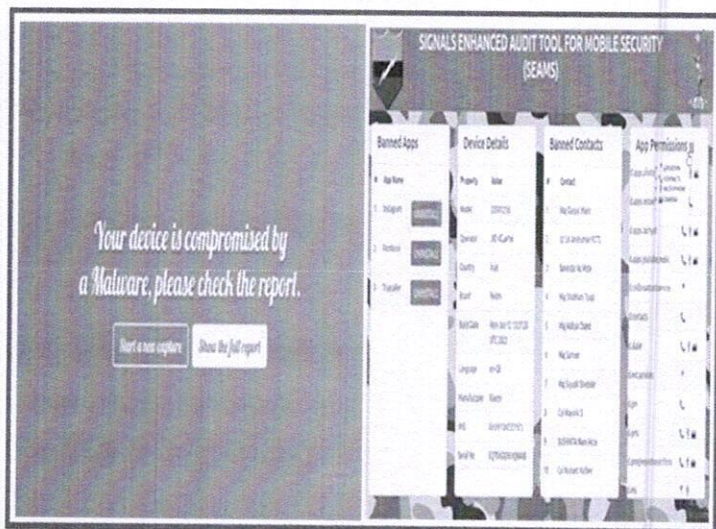
- i3 /i5 (depending on load).

(q) Enhancement up gradation (incl patch mgt sw spdt procedure and mechanism) -
Based on technological advancement, MCTE will provide upgrades.

(r) Recommendation, spl instrs and reqmt (if any) - NIL.

(s) Intended usage and dply –
(Standalone/LAN/ADN/Internet)

- Standalone with Internet connection



Annex II

(Ref Para 9(a) of DDG IT letter
No B/04001/Policy/Sw/ DDG IT
(T&P) dt 19 Jul 2022)

CHECKLIST: PRE APLV-STG**MANDATORY DETAILS**

1. Name of proj (incl ver) - PMSS
2. Name of sponsor - MCTE, MHOW
3. Type of Sw (Bespoke/ COTS/ Customized) - Customized
4. Brief justification for devp of Sw appl. -

PMSS combines cutting-edge AI and Deep Learning algorithms along with a signature-based detection engine to detect malicious network t/c emerging/converging from/to a smart device. It identifies malicious applications by analysing network activity from the scanned smart device. The scanning process takes only 3-4 minutes per device, producing real-time reports in three categories. Additionally, the appln enhances the cyber security by identifying and allowing one-click detection and removal of any banned applications on the smart device, thereby streamlining the cyber security assessment.
5. Aim & Scope Purpose incl utility, beneficiaries and tgt users -

To devp a AI based proactive mobile security sys in the units / fmn of IA
6. To be hosted on internet/ ADN with brief justification - Standalone with Internet contv
7. Being devp in house or through IT funds - In-house Devp
8. Usability of proposed appls by other arms / services / org/ est - All Units/ Fmn
9. Hw and IT infrastructure reqd -

(a) Windows 10 OS (desktop ver)

(b) For portable ver - Raspberry Pie, 10 inch display, 32 GB Memory Card
10. Brief details of content of the proposed Sw appl - complete mobile security sys for soldier
11. Endorsement by Head of Br/ Svc/ Fmn - MCTE
12. Details of user base - .exe file for usage

**IN PRINCIPAL APPROVAL OF DEPUTY COMMANDANT, FOR DEVELOPMENT
OF SOFTWARE (PMSS) BY CENTER OF EXPERTISE, ARTIFICIAL
INTELLIGENCE, MILITARY COLLEGE OF TELECOMMUNICATION
ENGINEERING, MHOW**

In Principal Approval for the development of AI based Proactive mobile security system software (PMSS) for vulnerability scanning and detection of banned application is here by accorded. The software will be useful in protecting the mobile phone of soldier in units/fmn.




Maj Gen
Deputy Commandant & CI
Military College of
Telecommunication Engineering