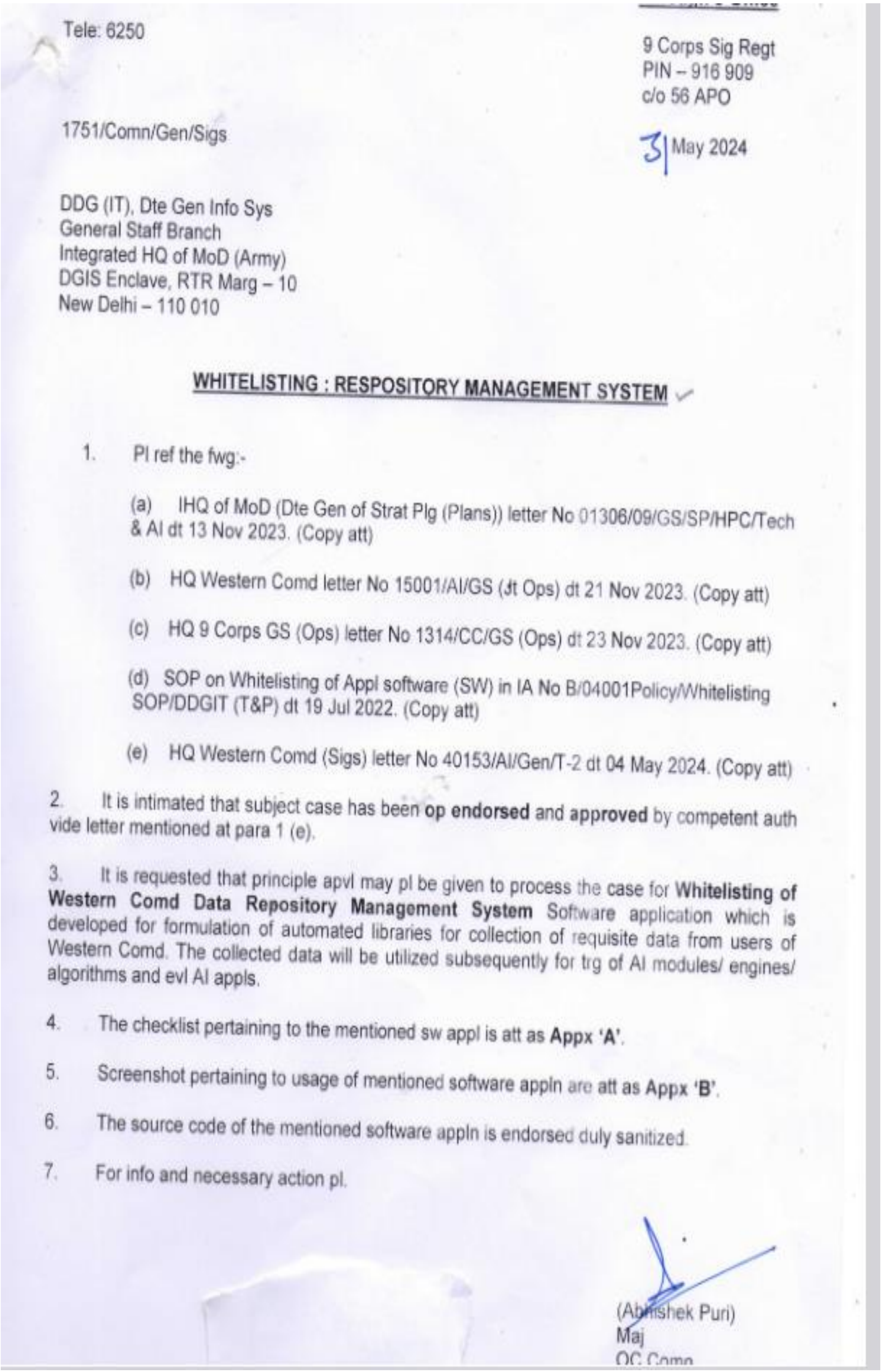


Tele: 6250

9 Corps Sig Regt
PIN – 916 909
c/o 56 APO

1751/Comn/Gen/Sigs

31 May 2024

DDG (IT), Dte Gen Info Sys
General Staff Branch
Integrated HQ of MoD (Army)
DGIS Enclave, RTR Marg – 10
New Delhi – 110 010

WHITELISTING : RESPOSITORY MANAGEMENT SYSTEM

1. Pl ref the fwg:-

(a) IHQ of MoD (Dte Gen of Strat Plg (Plans)) letter No 01306/09/GS/SP/HPC/Tech & AI dt 13 Nov 2023. (Copy att)

(b) HQ Western Comd letter No 15001/AI/GS (Jt Ops) dt 21 Nov 2023. (Copy att)

(c) HQ 9 Corps GS (Ops) letter No 1314/CC/GS (Ops) dt 23 Nov 2023. (Copy att)

(d) SOP on Whitelisting of Appl software (SW) in IA No B/04001Policy/Whitelisting SOP/DDGIT (T&P) dt 19 Jul 2022. (Copy att)

(e) HQ Western Comd (Sigs) letter No 40153/AI/Gen/T-2 dt 04 May 2024. (Copy att)

2. It is intimated that subject case has been **op endorsed** and **approved** by competent auth vide letter mentioned at para 1 (e).

3. It is requested that principle apvl may pl be given to process the case for **Whitelisting of Western Comd Data Repository Management System** Software application which is developed for formulation of automated libraries for collection of requisite data from users of Western Comd. The collected data will be utilized subsequently for trg of AI modules/ engines/ algorithms and evl AI appls.

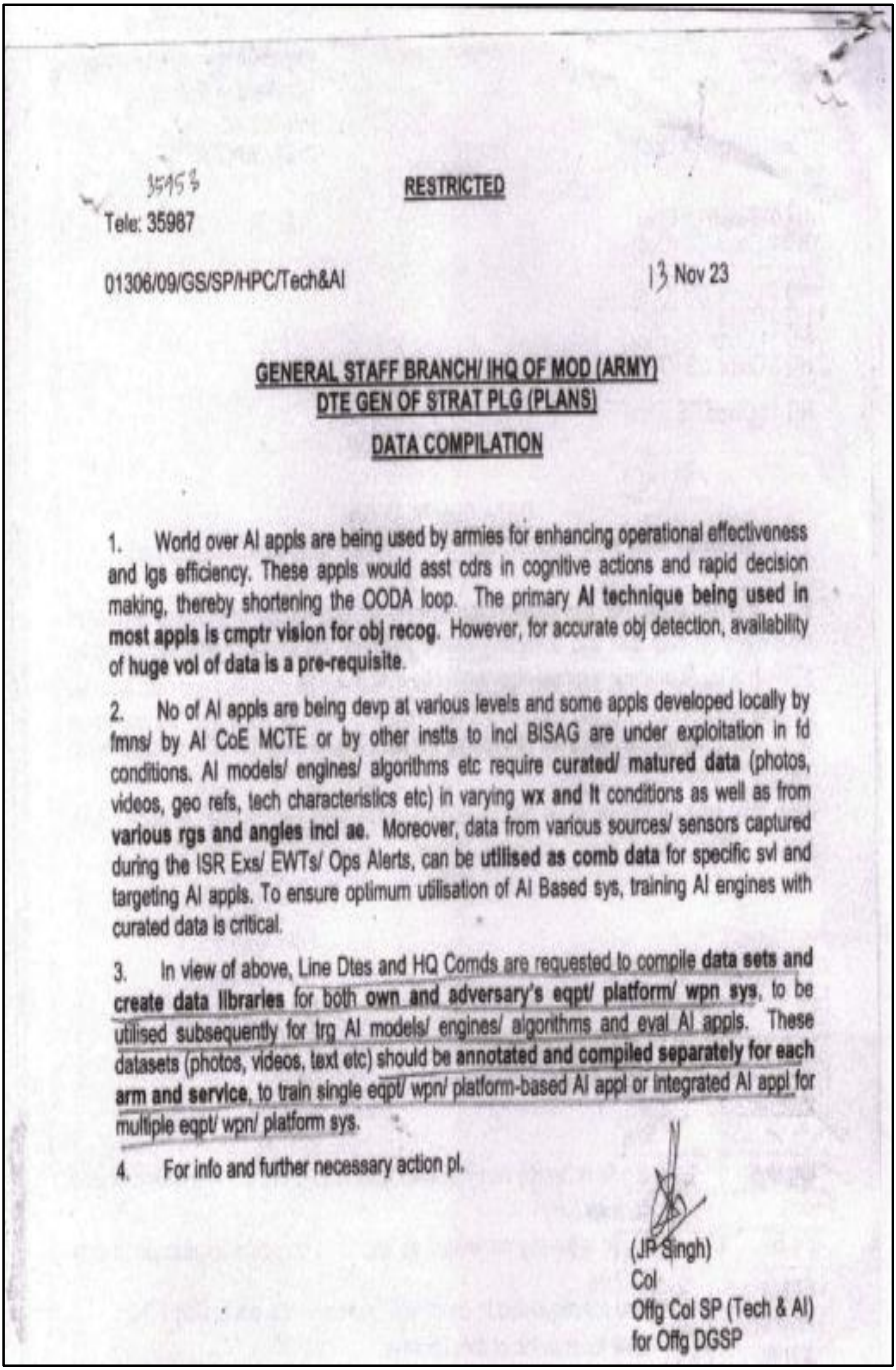
4. The checklist pertaining to the mentioned sw appl is att as **Appx 'A'**.

5. Screenshot pertaining to usage of mentioned software appln are att as **Appx 'B'**.

6. The source code of the mentioned software appln is endorsed duly sanitized.

7. For info and necessary action pl.

(Abhishek Puri)
Maj
OC Comn



35958

RESTRICTED

Tele: 35987

01306/09/GS/SP/HPC/Tech&AI

13 Nov 23

GENERAL STAFF BRANCH/ IHQ OF MOD (ARMY)
DTE GEN OF STRAT PLG (PLANS)

DATA COMPILATION

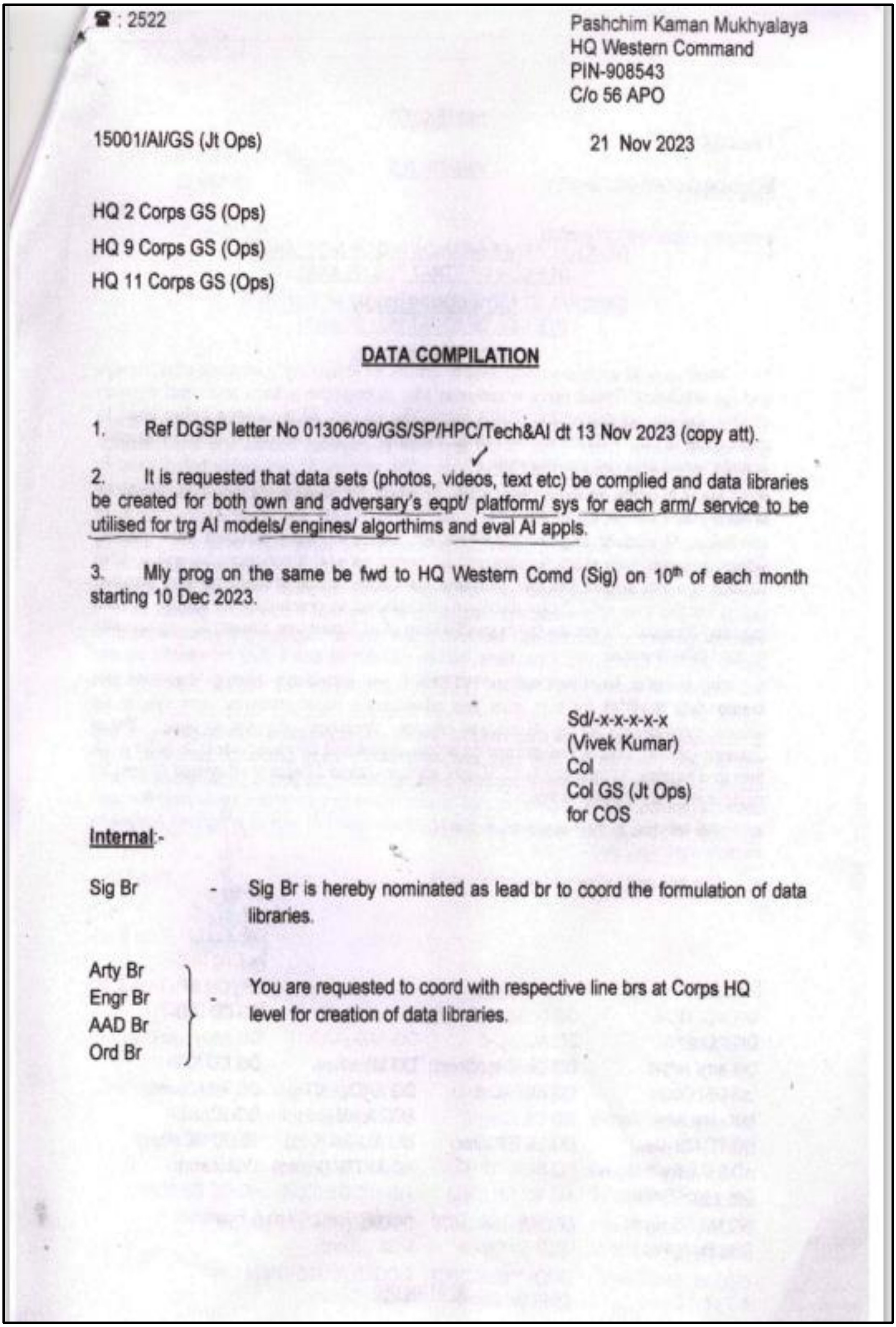
1. World over AI appls are being used by armies for enhancing operational effectiveness and lgs efficiency. These appls would asst cdrs in cognitive actions and rapid decision making, thereby shortening the OODA loop. The primary **AI technique being used in most appls is cmptr vision for obj recog.** However, for accurate obj detection, availability of **huge vol of data is a pre-requisite.**

2. No of AI appls are being devp at various levels and some appls developed locally by fmns/ by AI CoE MCTE or by other instts to incl BISAG are under exploitation in fd conditions. AI models/ engines/ algorithms etc require **curated/ matured data** (photos, videos, geo refs, tech characteristics etc) in varying **wx and lt** conditions as well as from **various rgs and angles incl ae.** Moreover, data from various sources/ sensors captured during the ISR Exs/ EWTs/ Ops Alerts, can be **utilised as comb data** for specific svl and targeting AI appls. To ensure optimum utilisation of AI Based sys, training AI engines with curated data is critical.

3. In view of above, Line Dtes and HQ Comds are requested to compile **data sets and create data libraries** for both **own and adversary's eqpt/ platform/ wpn sys**, to be utilised subsequently for trg AI models/ engines/ algorithms and eval AI appls. These datasets (photos, videos, text etc) should be **annotated and compiled separately for each arm and service**, to train single eqpt/ wpn/ platform-based AI appl or integrated AI appl for multiple eqpt/ wpn/ platform sys.

4. For info and further necessary action pl.

(JP Singh)
Col
Offg Col SP (Tech & AI)
for Offg DGSP



☎ : 2522

Pashchim Kaman Mukhyalaya
HQ Western Command
PIN-908543
C/o 56 APO

15001/AI/GS (Jt Ops)

21 Nov 2023

HQ 2 Corps GS (Ops)

HQ 9 Corps GS (Ops)

HQ 11 Corps GS (Ops)

DATA COMPILATION

1. Ref DGSP letter No 01306/09/GS/SP/HPC/Tech&AI dt 13 Nov 2023 (copy att).

2. It is requested that data sets (photos, videos, text etc) be complied and data libraries be created for both own and adversary's eqpt/ platform/ sys for each arm/ service to be utilised for trg AI models/ engines/ algorthims and eval AI appls.

3. Mly prog on the same be fwd to HQ Western Comd (Sig) on 10th of each month starting 10 Dec 2023.

Sd/-x-x-x-x-x
(Vivek Kumar)
Col
Col GS (Jt Ops)
for COS

Internal:-

Sig Br - Sig Br is hereby nominated as lead br to coord the formulation of data libraries.

Arty Br
Engr Br
AAD Br
Ord Br
- You are requested to coord with respective line brs at Corps HQ level for creation of data libraries.

२

☎ : 2626

1314/CC/GS (Ops) 23 Nov 2023

GS (OPS) BRANCH

DATA COMPILATION

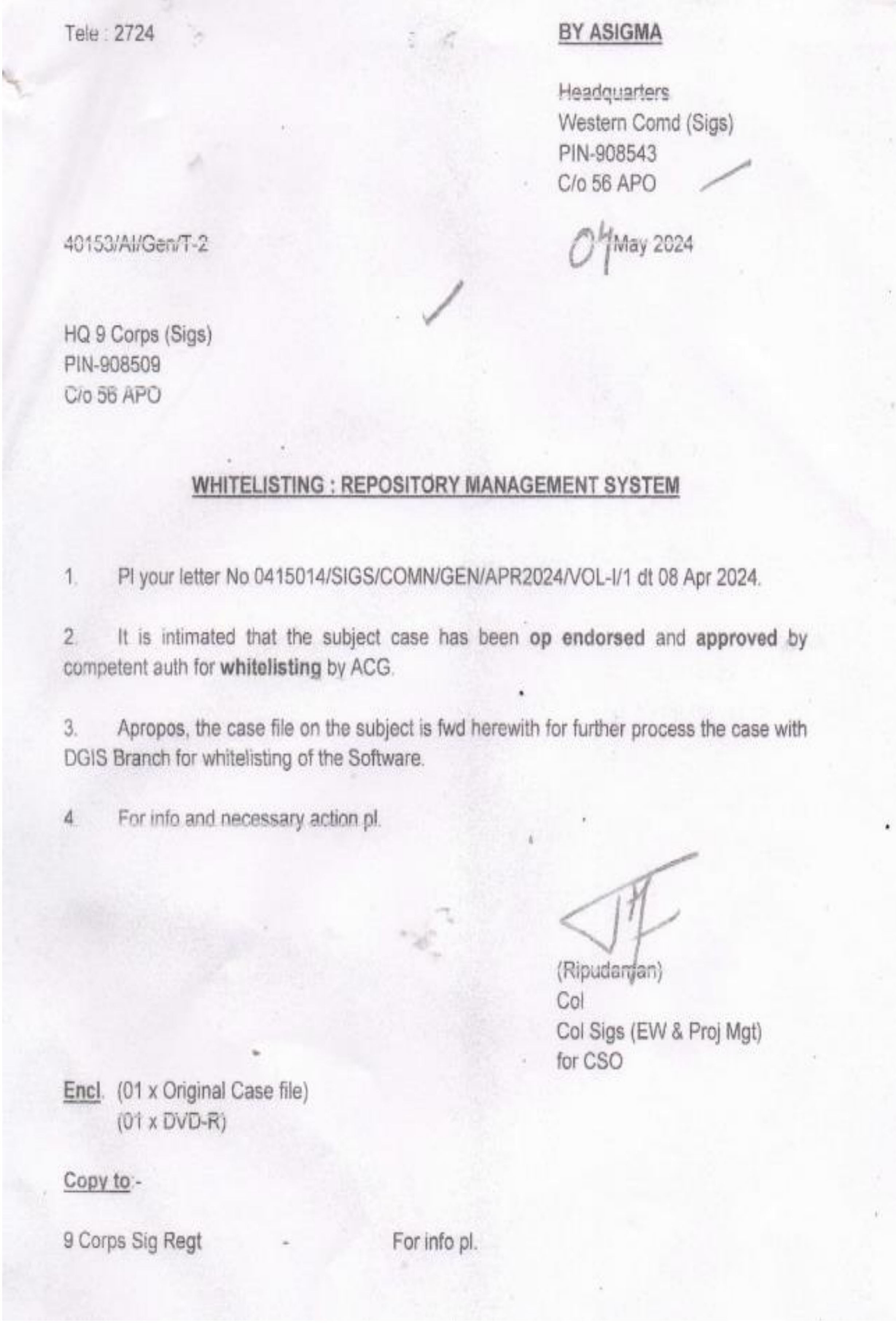
1. Ref HQ Western Comd letter No 15001/AI/GS (Jt Ops) dt 21 Nov 2023 (copy att).

2. Sigs br is hereby detailed as the nodal br to coord the formulation of data libraries. You are requested to fwd mly prog on the same to HQ Western Comd (Sig) on 10th of each month starting wef 10 Dec 2023 with info to this br.

(V Mahapatra)
Lt Col
GSO-1 (Ops) B

Encls : As above.

Sigs Branch



Tele : 2724

BY ASIGMA

Headquarters
Western Comd (Sigs)
PIN-908543
C/o 56 APO

40153/AI/Gen/T-2

04 May 2024

HQ 9 Corps (Sigs)
PIN-908509
C/o 56 APO

WHITELISTING : REPOSITORY MANAGEMENT SYSTEM

1. Pl your letter No 0415014/SIGS/COMN/GEN/APR2024/VOL-I/1 dt 08 Apr 2024.

2. It is intimated that the subject case has been **op endorsed** and **approved** by competent auth for **whitelisting** by ACG.

3. Apropos, the case file on the subject is fwd herewith for further process the case with DGIS Branch for whitelisting of the Software.

4. For info and necessary action pl.

(Ripudaman)
Col
Col Sigs (EW & Proj Mgt)
for CSO

Encl. (01 x Original Case file)
(01 x DVD-R)

Copy to:-

9 Corps Sig Regt - For info pl.

Appx 'A'

(Pl ref para 3 of 9 CSR letter No

1751/Comn/Gen/Sigs

dt ____ May 2024

CHECK LIST : PRE APVL STG

Ser No	Mandatory details	
1.	Name of Proj (incl ver)	Western Comd Repository Mgt Sys
2.	Name of sponsor	In-house
3.	Type of SW (Bespoke / COTS / Customized)	Bespoke
4.	Brief Justification / endorsement on reqmt for devp of Sw appl.	(a) Pl ref DGSP letter No 01306/09/GS/SP/HPC/Tech&AI dt 13 Nov 2023. (b) There is a reqmt to compile data sets and create data liberaries for both own and adversary's eqpt/ platform/ wpn sys, to be utilised subsequently for trg AI modules/ engines/ algorithms and eval AI appls. These datasets (Photos, videos, text etc) should be annotated and compiled separately for each arms and services to train single eqpt/ wpn/ platform-based AI appln or integrated AI appl for multiple eqpt/ wpn/ platform sys. To populate data all users of Western Comd need to injest datasheet in ibid appln.
5.	Aim & Scope purpose incl utility, beneficiaries and tgt users.	Br/Units (Comd/ Corps/ Div)
6.	To be hosted on internet / AND with brief justification	Yes, it will be hosted in UADN.
7.	Being devp in house or through IT funds.	In-house
8.	Usability of proposed appls by other arms/ Services/ Org/ est.	The application will be utilized by all Arms.
9.	Hw and IT infrastructure reqd.	Will be hosted on a server with centralized storage system.
10.	Berif details of content of the proposed Sw appl.	Data libraries for storage of data (own and adversary's eqpt/ platform/ wpn sys.

11.	Endorsement by Head of Br/ Svc/ Fmn.	HQ 9 Corps (Sigs) letter No 4125/Sigs/SD-1 dt 28 Nov 2023
12.	Details of user base.	All nominated appts of various HQ/ Fmn are reqd to populate the datasheet.

Addl details (optional in pre Apvl Stq: Mandatory in Posst Avpl Stq)		
13.	Envisaged cost of entire proj incl license fees and maint.	
14.	Projected dt of completion and tech maj timelines.	
15.	Brief details of Sw platform and tech stack proposed for devp of appl incl op sys dependencies (if any)	
16.	Brief details of proposed network and bandwith reqmts.	
17.	Brief details of OS & Sys software reqmts.	
18.	Brief details of proposed sate security measures incl backup of data.	
19.	Brief details of Proposed Database Engine To Be used in the Appl.	
20.	Detls of Sw architecture and COTS Sw proposed to be utilized.	
21.	Detls of Proposed architecture – Centralised / Federated/ Hybird.	
22.	Brief details of proposed utilization of Public Key infra (PKI) and iden and Access Mgt (IMA)	
23.	Technology dependencies (if any)	
24.	Database reqmts.	
25.	Enhancement/ upgradation (incl patch mgt/ Sw updt procedure and mechanism).	
26.	Details of licensing (if any)	

SOP ON WHITELISTING OF APPL SOFTWARE (SW) IN IA

Ref : –

(a) Army Cyber Security Policy- 2017.

(b) DGMO (MO-12) letter No A/12100/CSF/MO-12 dt 10 Aug 18.

(c) SOP on Whitelisting of Appl Software (SW) In IA issued by DDGIT vide B/04001/Policy/Whitelisting SOP/DDGIT (T&P) dt 20 May 20.

(d) DG Sigs letter No B/46850/IT/Sigs 7(a)/Policy dt 17 Feb 20.

(e) MO-12 letter No B/51153/ArCyGp/CSF/T-3 dt 20 Nov 20.

(f) DCOAS (IS&C) Sectt letter No 57926/ICT/DCOAS (IS&C) Sectt/IS dt 07 Sep 21.

(g) DGMO/ MO-12 letters No A/12108/Vetting/MO-12 dt 08 Oct 21 and 09 Mar 22.

(h) Mins of Mtg of 10th OAC held on 09 Jun 22.

INTRO

1. IT being a dynamic subject, reg/ frequent tech updt/ devps in Hardware and Sw have become a norm. Considering the wide footprint of IT in IA, there is an ever increasing reqmt of Sw appls for automation of various aspects of the org functioning.

2. The need for Sw appl is driven by users in IA and Sw appl proj are being undertaken by IA as in-house devp or outsourcing their devp to other Govt agencies/ trade. In addition, a number of COTS sw with/without customisation are reqd by the org. In order to ensure that devp efforts and resources are not wasted and benefit a larger user base, there is a definite need for all Sw appls to be scrutinised by a central agency, which has a larger visibility and understanding of the scope for pan-Army utility and dply.

AIM

3. To streamline the devp and use of all Sw appls in IA as also ensure that issues of security, relevance and pan-Army dply are facilitated.

SCOPE

4. DGIS and DG Sigs are the nodal agencies for whitelisting of web appls and websites respectively. While the whitelisting of websites is to be processed as per DG Sigs letter No B/46850/IT/Sigs 7(a)/Policy dt 17 Feb 2020, this SOP provides a framework for whitelisting of Sw appls (incl web appl, mob appl, Server Client Model appl, Standalone Desktop appl, COTS Sw appl etc) to be dply over standalone, exclusive LAN, ADN or Internet.

5. The subject is covered as follows: –

(a) **PART I** Gen Aspects.

(b) **PART II** Procedure for Whitelisting of Sw Devp In-House/ By Outsourcing to Govt Agencies/ Trade.

(c) **PART III** COTS Sw Appls.

(d) **PART IV** Timelines to be followed.

(e) **PART V** Salient aspects.

(f) **PART VI** Life Cycle Sp of Appl Devp by Sponsor Agencies.

PART I: GEN ASPECTS

6. **Nodal Agency**.

(a) DDG IT, DG IS will be the nodal agency for processing all cases for whitelisting of Sw appls less the ones to be whitelisted by DG Sigs (software/ appls for central services incl nw mgt, comn and nw security wrt ADN). Processing of case files, from sponsors to stakeholders and vice versa, will be through DDG IT. DDG IT will maint status of whitelisting of various Sw appls and will be repository of all whitelisted software. Accordingly, all agencies involved in the process must keep DDG IT info about the progress of whitelisting.

(b) **Whitelisting of Sw Appls for Central Services incl Nw Mgt, Comn and Nw Security wrt ADN**.

(i) All Sw appls for comn and nw mgt incl sw for centralised services on ADN will be whitelisted by DG Sigs, after its endorsement by DGMO / MO-10.

(ii) All Sw appls for ADN security will be whitelisted by DG Sigs, after its endorsement by DG MO / MO-12.

7. **Gen Pts**. Fwg pts will be adhered to by sponsor agencies before processing the case for whitelisting of Sw: –

(a) **Ownership**.

(i) Any Sw appl planned to be devp by any Fmn/ Est will be treated as the product (ownership) of the respective Fmn/ Est, incl data security and risk mgt aspects.

(ii) No IA pers shall host any Sw appl on Standalone PC/ exclusive LAN/ ADN/ Internet in indl capacity.

(b) **Endorsement for Reqmt of Sw Devp**. In order to minimise duplication of efforts, prior approval of respective Head of Br/ Svc/ Fmn will mandatorily be obtained by the sponsor.

(c) Appls already existing in the civ domain should be further devp/ refined by the Army instead of devp from scratch, ***provided it does not violate any IPR***.

(d) Considering impl of unified ADN in near future, cases for Sw appl planned to be dply over exclusive LAN are to be processed akin to dply on ADN and NOT exclusive LAN.

(e) Processing of Sw devp projs will be ensured as per DCOAS (IS&C) Sectt Note No 57926/ICT/DCOAS (IS&C) Sectt/IS dt 07 Sep 21 and in keeping with provns of DFPDS, GFR, DPM and IT SOP.

(f) **Sw Appls to be Hosted on Internet**. All such official Sw appls will have links on ADG SC maint IA web portal i.e. www.indianarmy.nic.in.

(g) **Adherence to Policies**. Sw devp will conform to policies/ instrs att as **Appx A** to this SOP.

(h) A presentation by the developer/ sponsor agency, if reqd, may be requested by any stake holder at any stg of processing of the case to understand the details of design, functionality and funding reqmts.

PART II: PROCEDURE FOR WHITELISTING OF SW DEVP IN-HOUSE/ BY OUTSOURCING TO GOVT AGENCIES/ TRADE

8. Procedure for whitelisting of Sw appls is divided into fwg stgs, flowchart for which is given at **Appx B** to this SOP: –

(a) Pre apvl stg.

(b) Post apvl stg.

(c) Post devp stg.

9. **Pre Apvl Stg**. This stg entails **In Principle Apvl** for the sponsor agency to further process the case file.

(a) Sponsor agency to fwd duly completed checklist, att as **Appx C**, to DDG IT by ASIGMA.

(b) To avoid dupl of effort and resources, sponsor agency will process the case only if similar Sw is not mentioned in the list of whitelisted Sw appls or in the list of Sw appls under process for whitelisting, available on DDG IT website on ADN.

(c) **Sw Appls to be Hosted on Internet**. Fwg will be adhered to by the sponsor: –

(i) Fwg details, **in addn to Appx C**, will also be incl in the case file: –

(aa) Op need incl reasons for hosting the appl on Internet, rather than secure air-gapped service Nws.

(ab) Clearly defined data ownership and data safety responsibility wrt info planned to be hosted on the Internet.

(ac) Degree of risk recom to be accepted in case of compromise of the appl.

(ad) Single pt contact for Sw appl.

(ii) All Internet based appls will be devp as mob handset friendly web appl instead of mob APK to obviate the inherent vulns associated with mob appl.

(d) **Automation Committee**. DDG IT will ref cases received as above to **appropriate Automation Committees, starting with Steering Automation Committee (SAC) for apvl**. *MI-11 rep is reqd to attend such mtgs in SAC as Spl Invitee.*

(e) **In Principle Approval** will be accorded by relevant Automation Committee as per fwg parameters: –

(i) **Steering Automation Committee (SAC)**. Upto Rs 50 Lakhs.

(ii) **Oversight Automation Committee (OAC)**. Above Rs 50 lakhs and below Rs 5 Crs.

(iii) **Empowered Automation Committee (EAC)**. Above Rs 5 Crs.

(f) **Resp of Stakeholders During Automation Committees**

(i) **DDG IT**. To vet the Sw appl proposal from dupl and utility pt of view.

(ii) **DG MO (IW)**. Cyber Security aspects.

(iii) **DG Sigs**. Network, bandwidth, OS & Hw resources (servers) aspects.

10. **Post Apvl Stg.** On receipt of In Principle Apvl, sponsor agency will proceed as follows: –

(a) **Fin Sp for Sw Devp**. Funds reqd for apvd appls may be projected to respective High-Level Budget Holder (HLBH) by the sponsor agency for inclusion in IT PPP.

(b) **Proj Devp & Mgt Gp (PDMG)**

(i) A PDMG will be formed under the aegis of the sponsor agency to ensure the fwg: –

(aa) Est the ownership of Sw.

(ab) Prep of a comprehensive case file and forwarding it to DG IS (DDG IT) for vetting by ASDC, AHCC, MI-11 and ACG.

(ac) Reg monitoring of the prog of proj and fwd feedback to DDG IT in case of change in scope or reqmt of addl funding (only in cases where DDG IT is the HLBH).

(ad) Mgt of the Sw appl throughout its entire lifecycle (details at Para 15 below).

(ae) ACG may be considered for incorporating as part of PDMG only for enterprise/ maj pan IA level Sw devp projs ***till RFP stg only***. Guidance wrt cyber security aspects from MO-12/ ACG may be solicited for all other Sw being devp in IA to ensure faster impl.

(c) **Processing of Case File**. Sponsor agency to fwd case file along with fwg docus to DDG IT: –

(i) **Checklist**. Details mentioned as **'Optional'** in **Appx C** will now mandatorily be included in case file for processing it in this stg.

(ii) In cases of Sw devp through IT funds: –

(aa) S of C as per DPM - 2009 and amdts thereto.

(ab) Draft RFP.

(d) DDG IT will process the case file for clearances as follows: –

(i) **Sw Appls to be Hosted on ADN/ LAN/ Internet**. DDG IT → ASDC → AHCC → ACG.

(ii) **Sw Appls to be Hosted on Stand Alone PC.** DDG IT→ASDC→ACG.

(e) **Resp of Stake Holders**

(i) **DDG IT**.

(aa) Process the case file for clearance by stakeholders and according apvl to sponsor agency for proceeding with devp of Sw appl.

(ab) Budgetary sp for devp of Sw appl.

(ii) **ASDC**. To analyse the Sw appl proposal with respect to the fwg: –

(aa) Platform being used.

(ab) Database to be used.

(ac) Sw architecture to incl Sw being used & COTS Sw dependencies.

(ad) Integration reqmt with other Sws (Offline/Online).

(ae) Usability of Sw by other arms/services/fmns/orgs.

(iii) **AHCC**.

(aa) For clearance with respect to architecture planned, Hw & IT Infrastructure, Nw usage reqmts and bandwidth utilisation.

(ab) Integrating the appl to be dply on ADN with Iden and Access Mgt (IAM) framework for role based access shall be a mandatory pre-requisite. However, integration with Public Key Infra (PKI), for added security can be undertaken if reqd.

(ac) Data storage reqmts & policy wrt data security, backup & ownership of data.

(iv) **ACG**. Vetting of case file and draft RFP of the proposed appl from cyber security perspective.

(f) **SAC will monitor timely processing of case files by all stakeholders.**

(g) Sponsor agency to proceed with devp of Sw appl only after the case file is cleared by DDG IT in post apvl stg.

11. **Post Devp Stg**. Once the Sw appl has been devp by the sponsor agency, sequence of action will be as follows: –

(a) Sponsor agency to coord with MI-11 for content vetting of Sw appl by them.

(b) Sponsor agency to fwd final Sw Appl (VDI/ Executable Image) as follows: –

(i) **AHCC**. For validation of the dply architecture, authentication, security overlays and BW reqmts of Sw appl to be hosted on ADN, as apvd initially during vetting stage. Confirmatory trials/ test bed setup may be reqd for specific cases for validating architecture/ BW/ data services reqmts on apvl of MO Dte, one appl at a time.

(ii) **ACG**. For cyber security clearance specific to the dply scenario.

(iii) **Cyber Security Clearance from Cert-In in Case of Sw Appls to be Hosted on Internet**. In case of Sw appls to be hosted on internet, cyber security clearance will be obtained from Cert-In by the sponsor agency before submitting the Virtual Disk Image (VDI)/ executable image of Sw appl to ACG.

(iv) Sponsor agency to submit final Sw appl (VDI/ Executable Image) to DG IS (DDG IT) along with copy of Cert In, MI-11, AHCC and ACG clearances.

(v) DG IS (DDG IT) incls Sw appl in list of Whitelisted Sw and promulgates same to envt.

(c) **Hosting of Sw Appl**. Sw appl will be hosted as follows **only after it has been whitelisted by DG IS (DDG IT)**: –

(i) **On ADN**. Sponsor agency to submit final Sw appl (VDI/ Executable Image) to AHCC for hosting and remote testing of ACG.

(ii) **On NIC (Internet)**. Sponsor agency to coord with AHCC for DNS regn and hosting on NIC.

(iii) **On Exclusive LAN / Standalone PC**. By sponsor agency.

PART III: COTS SW APPLS

12. Sub cat of COTS Sw and procedure to be followed for each is as follows: –

S No	Type of COTS Sw	Procedure	Remarks
(a)	Sw appls reqd for specific purposes like security tools and Sw devp, utilised by ACG and ASDC respectively.	Case for **permission** to use such Sw appl will be fwd to DDG IT for further processing with ASDC, ACG and DG Sigs.	***Permission so accorded*** (i) ***Will only be valid for specific dply scenario*** and reqmt as projected by the sponsor. Any variation from same would necessitate fresh permission. *(ii) Patch mgt of all COTS Sw on ADN will be centrally managed by DG Sigs and that dply in standalone mode will be managed by the sponsor.* (iii) **Will not be treated as auth for proc.**
(b)	COTS Sw appls proposed to be proc with or w/o source code, and ***utilised as such***/ customized by users in IA.		

13. **Selection of COTS Sw**. The sponsor should convene a Bd of qualified offrs who need to assess COTS Sw appls with respect to fwg parameters, to select the most suitable one: –

(a) **Availability of Source Code**. Source codes for bespoke/ customised Sw appls should be made available to the sponsor Unit/ Est / Fmn by the vendor.

(b) **Feasibility of Offline Dply**. In case of ADN/ LAN appl, the COTS Sw should be able to dply on IA Nw in offline envt without using any internet based services or related envt. All the dependencies should be included in the setup and installed along with the Sw without the reqmt of the internet.

(c) **Centralised Auto Updating and Patch Mgt**. The updation and patching of the Sw dply on ADN is carried out through the domain controllers at different levels. Any COTS Sw to be dply on ADN should be compatible and be able to receive upts and patches through existing centralized infrastructure.

(d) **Frequency and Regularity of Upts and Security Patches**. The appl will need periodic and regular patch mgt vis-à-vis the CVEs of the Sw comp used in the appl. This activity has to be promptly undertaken by the devp/ sys admin to ensure the appl vulnerabilities are patched imdt. To ensure that the appl is up to date, regular updation of the appl should be carried out. The COTS Sw with reg & faster rel of updates/ security patches should be given preference.

(e) **User Base**. It is imp that the COTS Sw selected should have a wider user base with high customer rating which will ensure better user confidence in the Sw.

(f) **End of Life and End of Sp**. Upon reaching its end of useful life, the OEM should provide the Sw sp in form of tech sp, risk analysis of its comp and its procedural mitigation, overall up gradation of the Sw and its related services. Therefore, Sw with higher EoL & EoS should be preferred.

(g) **OEM reputation**. The OEM company size and turnover should be considered as it shows the capb of the company to provide resources and sp for the COTS Sw efficiently as and when reqd w/o any delay in the service.

(h) **Date Breaches and Compromise**. History of attks & CVEs found in other Sw devp by OEM in the past or currently in user should be considered so as to understand the security threats & also the steps taken by the company to know its Incident Response capb.

(j) **PII Collected**. The PII data can be used to create a user profile. To ensure that the info related to the user is secured, the data collected by the OEM should be encoded and its usages be defined clearly at all levels. The data being entered in the sys must have adequate validations and it must be ensured that the file upload or remote code execution vulnerabilities are non-existent in the designed Sw. Min & non-cl PII data should be collected by the Sw.

(k) **Eval under Common Criteria**. For those Sw products which have been eval under CC, the initial selection of vendors can be based on desired Eval Assurance Levels (EAL) by the client. The final selection of vendor should be made by matching the client's desired Protection Profiles (PPs) with the Security Targets (STs) provided by the vendors.

PART IV: TIMELINES TO BE FOLLOWED

14. **Timelines For Clearances**. Timelines for according clearances to the Sw appls (in case there are no obsns) is as under: –

(a)	DDG IT	-	01 week.
(b)	ASDC	-	01 week.
(c)	DG Sigs	-	02 weeks.
(d)	MI-11	-	01 week
(e)	ACG	-	04 weeks.

PART V: SALIENT ASPECTS

15. Salient aspects of whitelisting of Sw appls are as follows: –

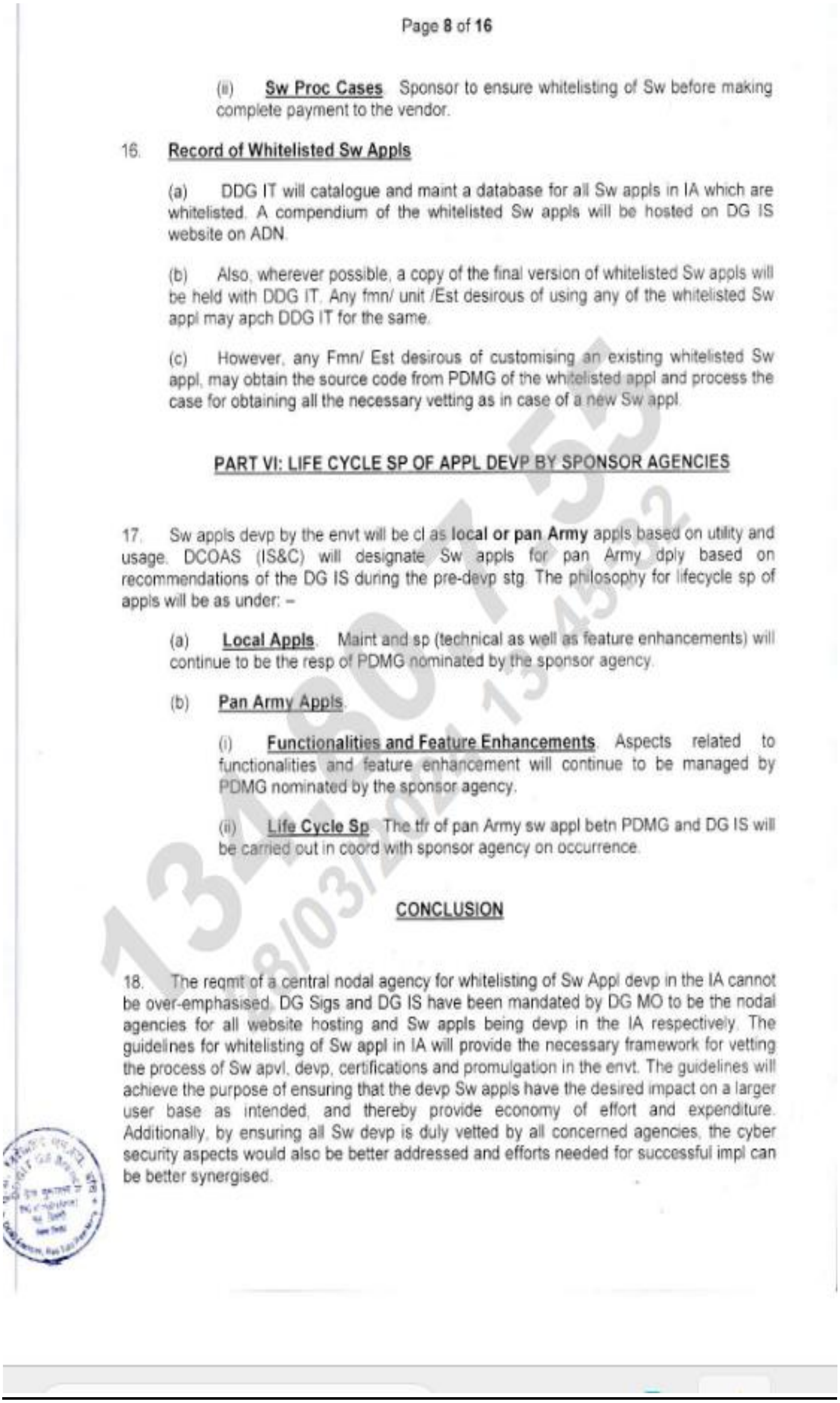
(a) **Validity**

(i) Since Cyber security clearance accorded to an appl is valid for a pd one yr and three yr for Sw appls to be hosted on internet and ADN/ LAN/ Stan Alone respectively, whitelisting of Sw appl will accordingly be valid for same duration from the dt of issue.

(ii) Sponsor agency will again process case with DDG IT for whitelisting in case of any update/ changes/ mod/ expiry of validity of the whitelisted Sw appl.

(b) **Payment Terms**. Sponsor may suitably incorporate fwg in the RFP: –

(i) **Sw Devp Cases**. Payment to vendor should be linked with suitable milestones of Sw devp and cyber security vetting.



(ii) **Sw Proc Cases**. Sponsor to ensure whitelisting of Sw before making complete payment to the vendor.

16. **Record of Whitelisted Sw Appls**

(a) DDG IT will catalogue and maint a database for all Sw appls in IA which are whitelisted. A compendium of the whitelisted Sw appls will be hosted on DG IS website on ADN.

(b) Also, wherever possible, a copy of the final version of whitelisted Sw appls will be held with DDG IT. Any fmn/ unit /Est desirous of using any of the whitelisted Sw appl may apch DDG IT for the same.

(c) However, any Fmn/ Est desirous of customising an existing whitelisted Sw appl, may obtain the source code from PDMG of the whitelisted appl and process the case for obtaining all the necessary vetting as in case of a new Sw appl.

PART VI: LIFE CYCLE SP OF APPL DEVP BY SPONSOR AGENCIES

17. Sw appls devp by the envt will be cl as **local or pan Army** appls based on utility and usage. DCOAS (IS&C) will designate Sw appls for pan Army dply based on recommendations of the DG IS during the pre-devp stg. The philosophy for lifecycle sp of appls will be as under: –

(a) **Local Appls**. Maint and sp (technical as well as feature enhancements) will continue to be the resp of PDMG nominated by the sponsor agency.

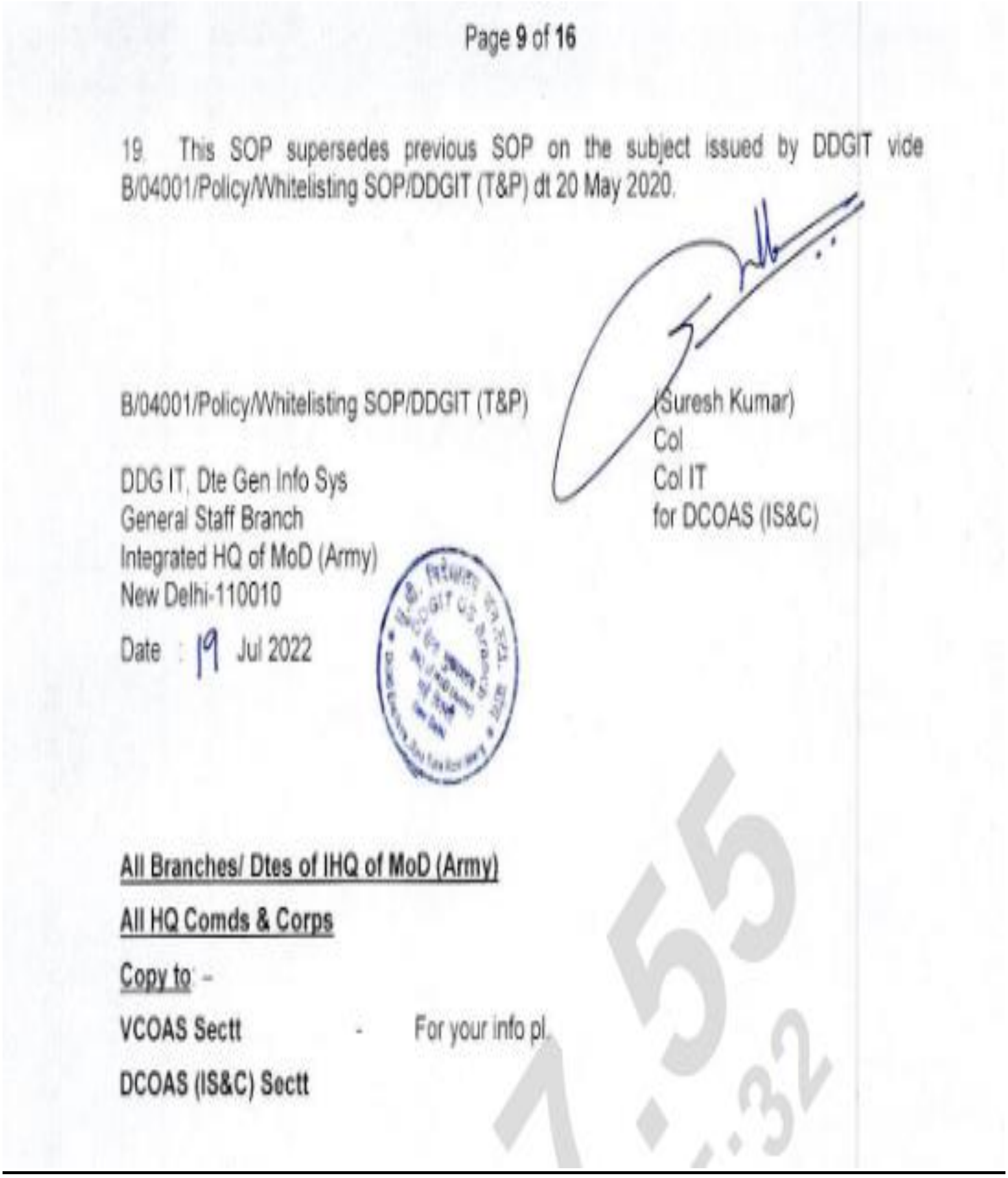
(b) **Pan Army Appls**.

(i) **Functionalities and Feature Enhancements**. Aspects related to functionalities and feature enhancement will continue to be managed by PDMG nominated by the sponsor agency.

(ii) **Life Cycle Sp**. The tfr of pan Army sw appl betn PDMG and DG IS will be carried out in coord with sponsor agency on occurrence.

CONCLUSION

18. The reqmt of a central nodal agency for whitelisting of Sw Appl devp in the IA cannot be over-emphasised. DG Sigs and DG IS have been mandated by DG MO to be the nodal agencies for all website hosting and Sw appls being devp in the IA respectively. The guidelines for whitelisting of Sw appl in IA will provide the necessary framework for vetting the process of Sw apvl, devp, certifications and promulgation in the envt. The guidelines will achieve the purpose of ensuring that the devp Sw appls have the desired impact on a larger user base as intended, and thereby provide economy of effort and expenditure. Additionally, by ensuring all Sw devp is duly vetted by all concerned agencies, the cyber security aspects would also be better addressed and efforts needed for successful impl can be better synergised.



19. This SOP supersedes previous SOP on the subject issued by DDGIT vide B/04001/Policy/Whitelisting SOP/DDGIT (T&P) dt 20 May 2020.

B/04001/Policy/Whitelisting SOP/DDGIT (T&P)

(Suresh Kumar)
Col
Col IT
for DCOAS (IS&C)

DDG IT, Dte Gen Info Sys
General Staff Branch
Integrated HQ of MoD (Army)
New Delhi-110010

Date : 19 Jul 2022

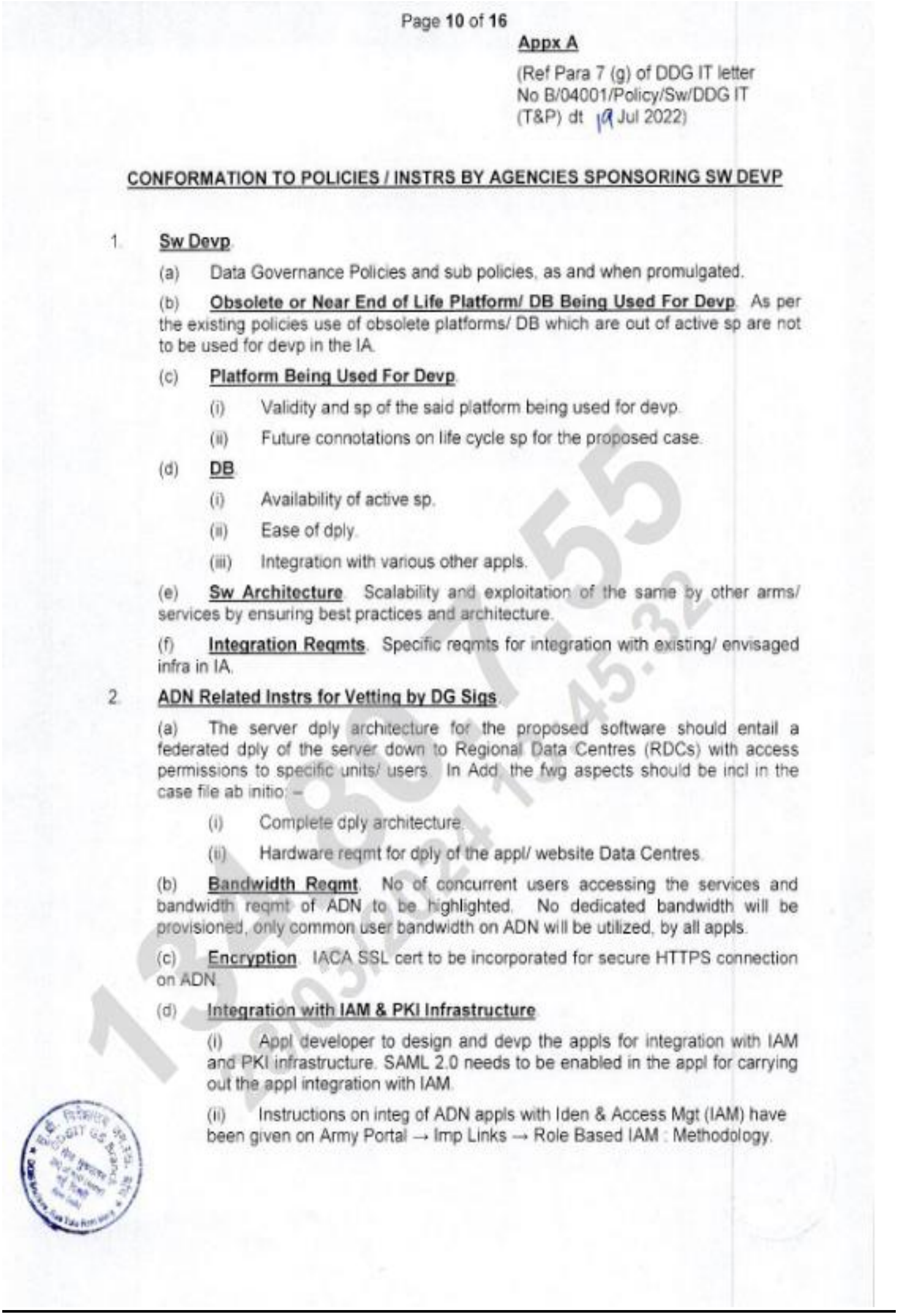
All Branches/ Dtes of IHQ of MoD (Army)

All HQ Comds & Corps

Copy to: -

VCOAS Sectt - For your info pl.

DCOAS (IS&C) Sectt



Appx A

(Ref Para 7 (g) of DDG IT letter
No B/04001/Policy/Sw/DDG IT
(T&P) dt 19 Jul 2022)

CONFORMATION TO POLICIES / INSTRS BY AGENCIES SPONSORING SW DEVP

1. **Sw Devp**.

(a) Data Governance Policies and sub policies, as and when promulgated.

(b) **Obsolete or Near End of Life Platform/ DB Being Used For Devp**. As per the existing policies use of obsolete platforms/ DB which are out of active sp are not to be used for devp in the IA.

(c) **Platform Being Used For Devp**.

(i) Validity and sp of the said platform being used for devp.

(ii) Future connotations on life cycle sp for the proposed case.

(d) **DB**.

(i) Availability of active sp.

(ii) Ease of dply.

(iii) Integration with various other appls.

(e) **Sw Architecture**. Scalability and exploitation of the same by other arms/ services by ensuring best practices and architecture.

(f) **Integration Reqmts**. Specific reqmts for integration with existing/ envisaged infra in IA.

2. **ADN Related Instrs for Vetting by DG Sigs**.

(a) The server dply architecture for the proposed software should entail a federated dply of the server down to Regional Data Centres (RDCs) with access permissions to specific units/ users. In Add, the fwg aspects should be incl in the case file ab initio: –

(i) Complete dply architecture.

(ii) Hardware reqmt for dply of the appl/ website Data Centres.

(b) **Bandwidth Reqmt**. No of concurrent users accessing the services and bandwidth reqmt of ADN to be highlighted. No dedicated bandwidth will be provisioned, only common user bandwidth on ADN will be utilized, by all appls.

(c) **Encryption**. IACA SSL cert to be incorporated for secure HTTPS connection on ADN.

(d) **Integration with IAM & PKI Infrastructure**.

(i) Appl developer to design and devp the appls for integration with IAM and PKI infrastructure. SAML 2.0 needs to be enabled in the appl for carrying out the appl integration with IAM.

(ii) Instructions on integ of ADN appls with Iden & Access Mgt (IAM) have been given on Army Portal → Imp Links → Role Based IAM : Methodology.

(e) To address emerging security threats, Port reqmt of each appl will be finalised in consultation with DG Sigs (Sigs-7). All services envisaged by the appl will be highlighted at vetting stg. Further, any changes in the rules / policies / ports reqd to be done in firewall / IPs be specified along with wk flow. Appls must utilise only auth ports approved for the appl. These ports should be mandatorily limited to the barest min reqd.

(f) **VAPT**. Appl developer should mitigate all vulnerabilities raised during audit by ACG.

(g) **Meta Tags**. All relevant meta tags to be filled in to make the appl Sw more descriptive and searchable.

(h) Appl to share data with Data Warehouse through API gateways.

(j) **Routing Protocol**. Comply with all ADN routing protocols of all tfc generated by the appl on ADN.

3. **Content Vetting by MI-11**.

(a) Provision of AR-21 and Para 322 of RA, Revised Edn 1987 and Para 11 & 12 of SAO 3/S/2001/MI will be strictly complied with.

(b) No cl info will be divulged/ issued/ hosted.

(c) **Office Responsibility**. Para 23 of SAO 3/S/2001/MI states, "The granting of permission to the publication of an article, a look, delivery of a lecture, broadcast or telecast does not convey official endorsement of its content. No statement implying such apvl, endorsement or permission will be included in any part of the material".

(d) NOC & Author Cert as per Para 21 of SAO 3/S/2001/MI be submitted to DG MI/MI-11 before hosting the data.

(e) No Cl/ Sensitive info to be shared to be uploaded.

(f) ORBAT detls in any form should not be revealed or asked for.

(g) Strong access cont mechanism should be based on the **Need to Know** basis.

(h) Role based access should be based on the mandated/ authorised appt accessing the appl.

(j) Adequate & latest encryption to prevent any malware/ phishing attks.

4. **Cyber Security Vetting**. Fwg policies promulgated by DGMO to be adhered to: –

(a) Appl Security: Evolving User Requirement Document (URD).

(b) Cyber security parameters to be checked by Cert-In Empaneled Auditor for websites and web appls hosted on internet.

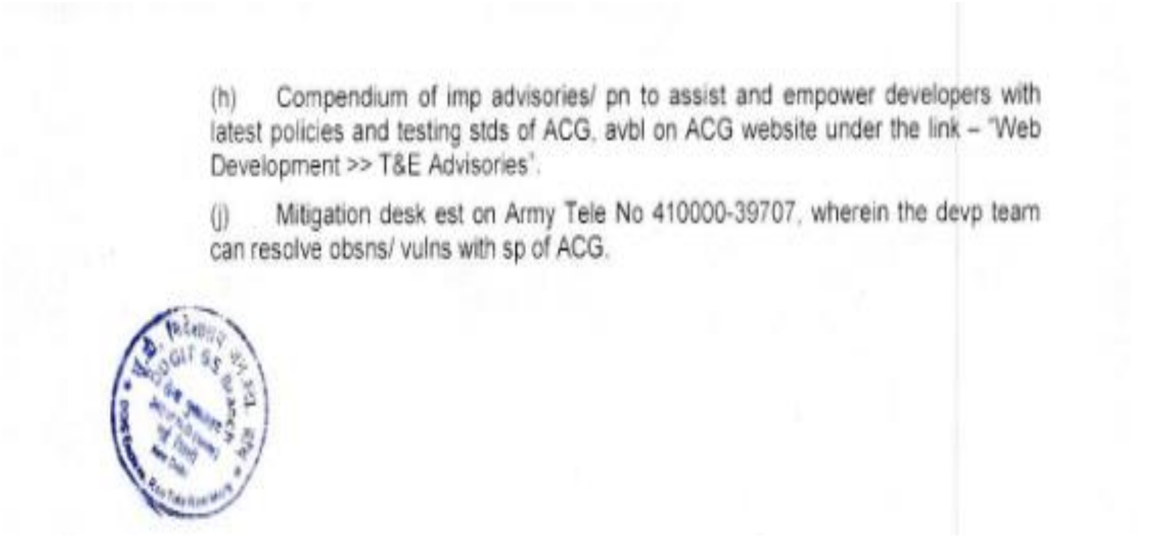
(c) DG MO/MO-12 letter No A/12108/Vetting/MO12 dt 13 Sep 2021 on "Impl Instrs: Internet Framework for IA".

(d) DG MO/MO-12 letter No A/12108/Vetting/MO12 dt 21 Sep 2021 on "Guidelines for Expediting Vetting of Websites/ Web Appl".

(e) DG MO/MO-10 letter No A/90222/MO-10/102 dt 06 Sep 2021 on "Revision of Policy: Software Encryption Secured Appls".

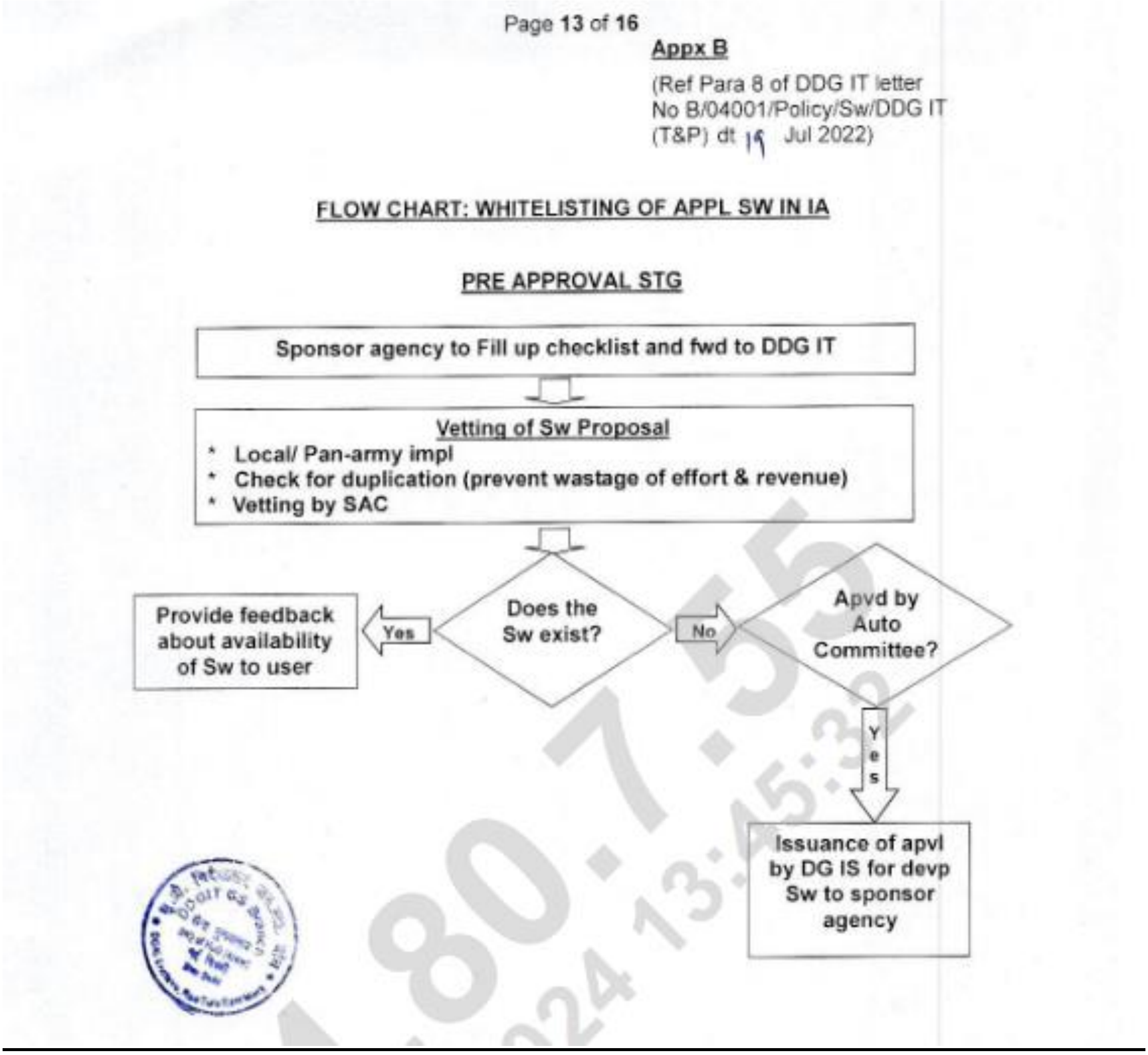
(f) DG MO/MO-10 letter No A/90213/MO-10/11 dt 09 Sep 2021 on "Unified ADN: Revision of Policies".

(g) DG MO/MO-10 letter No A/90222/MO-10/107 dt 24 Dec 2020 on "Data Governance Policy for IA: 2020" and various sub policies promulgated by DG Sigs and DG IS.



(h) Compendium of imp advisories/ pn to assist and empower developers with latest policies and testing stds of ACG, avbl on ACG website under the link – "Web Development >> T&E Advisories'.

(j) Mitigation desk est on Army Tele No 410000-39707, wherein the devp team can resolve obsns/ vulns with sp of ACG.



Appx B

(Ref Para 8 of DDG IT letter
No B/04001/Policy/Sw/DDG IT
(T&P) dt 19 Jul 2022)

FLOW CHART: WHITELISTING OF APPL SW IN IA

PRE APPROVAL STG

Sponsor agency to Fill up checklist and fwd to DDG IT

Vetting of Sw Proposal

* Local/ Pan-army impl

* Check for duplication (prevent wastage of effort & revenue)

* Vetting by SAC

Does the Sw exist?

Yes

Provide feedback about availability of Sw to user

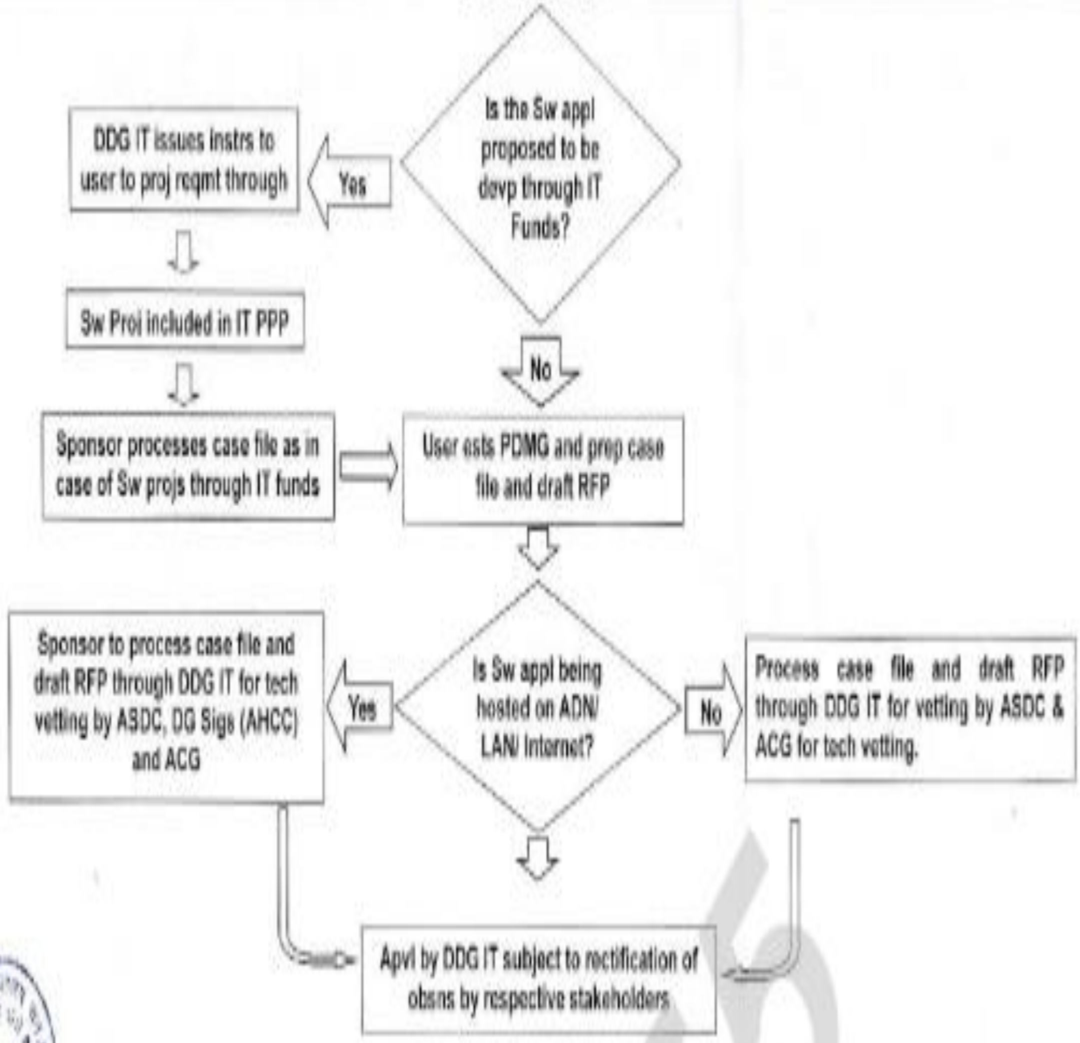
No

Apvd by Auto Committee?

Yes

Issuance of apvl by DG IS for devp Sw to sponsor agency

POST APVL STG



Is the Sw appl proposed to be devp through IT Funds?

Yes

DDG IT issues instrs to user to proj reqmt through

Sw Proj included in IT PPP

Sponsor processes case file as in case of Sw projs through IT funds

No

User ests PDMG and prep case file and draft RFP

Is Sw appl being hosted on ADN/ LAN/ Internet?

Yes

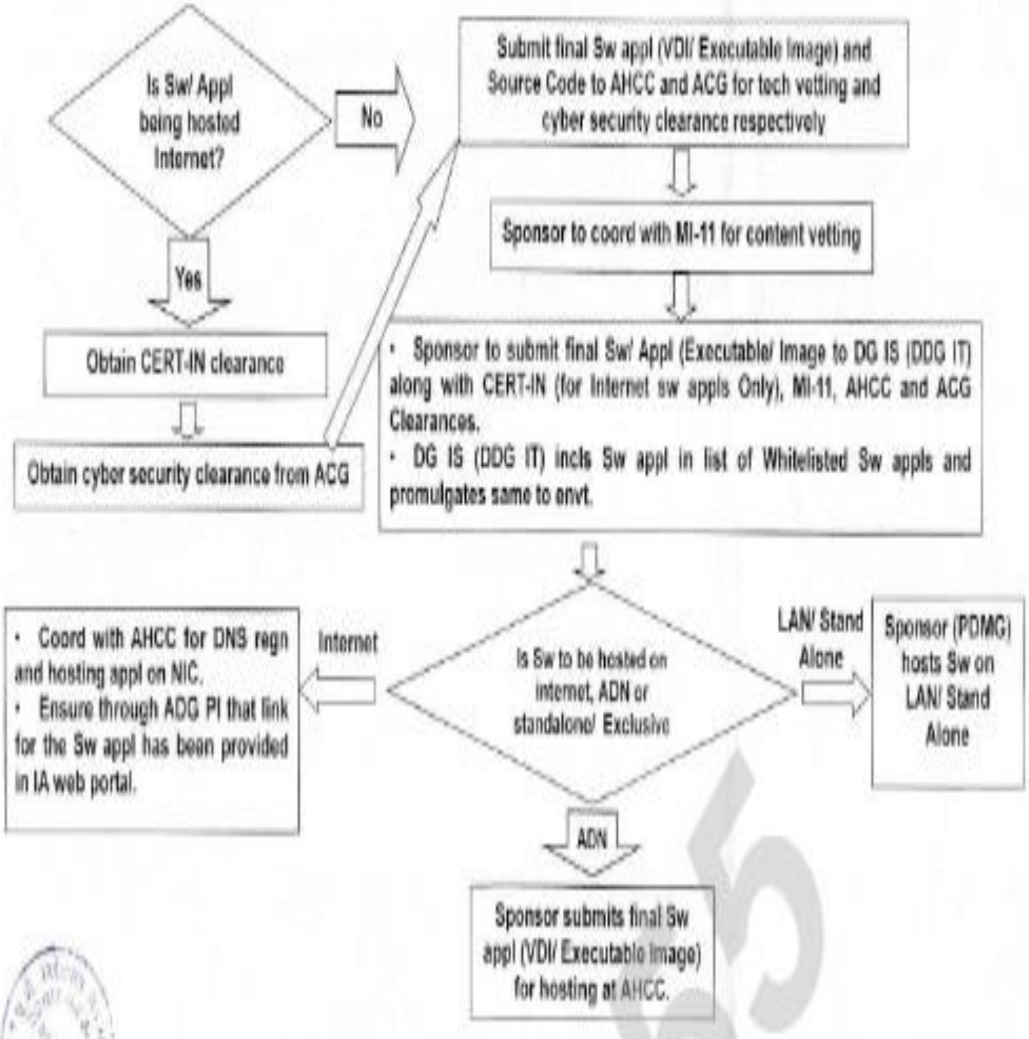
Sponsor to process case file and draft RFP through DDG IT for tech vetting by ASDC, DG Sigs (AHCC) and ACG

No

Process case file and draft RFP through DDG IT for vetting by ASDC & ACG for tech vetting.

Apvl by DDG IT subject to rectification of obsns by respective stakeholders

POST DEVP STG



Is Sw/ Appl being hosted Internet?

No

Submit final Sw appl (VDI/ Executable Image) and Source Code to AHCC and ACG for tech vetting and cyber security clearance respectively

Sponsor to coord with MI-11 for content vetting

Yes

Obtain CERT-IN clearance

Obtain cyber security clearance from ACG

- Sponsor to submit final Sw/ Appl (Executable/ Image to DG IS (DDG IT) along with CERT-IN (for Internet sw appls Only), MI-11, AHCC and ACG Clearances.
- DG IS (DDG IT) incls Sw appl in list of Whitelisted Sw appls and promulgates same to envt.

Is Sw to be hosted on internet, ADN or standalone/ Exclusive

Internet

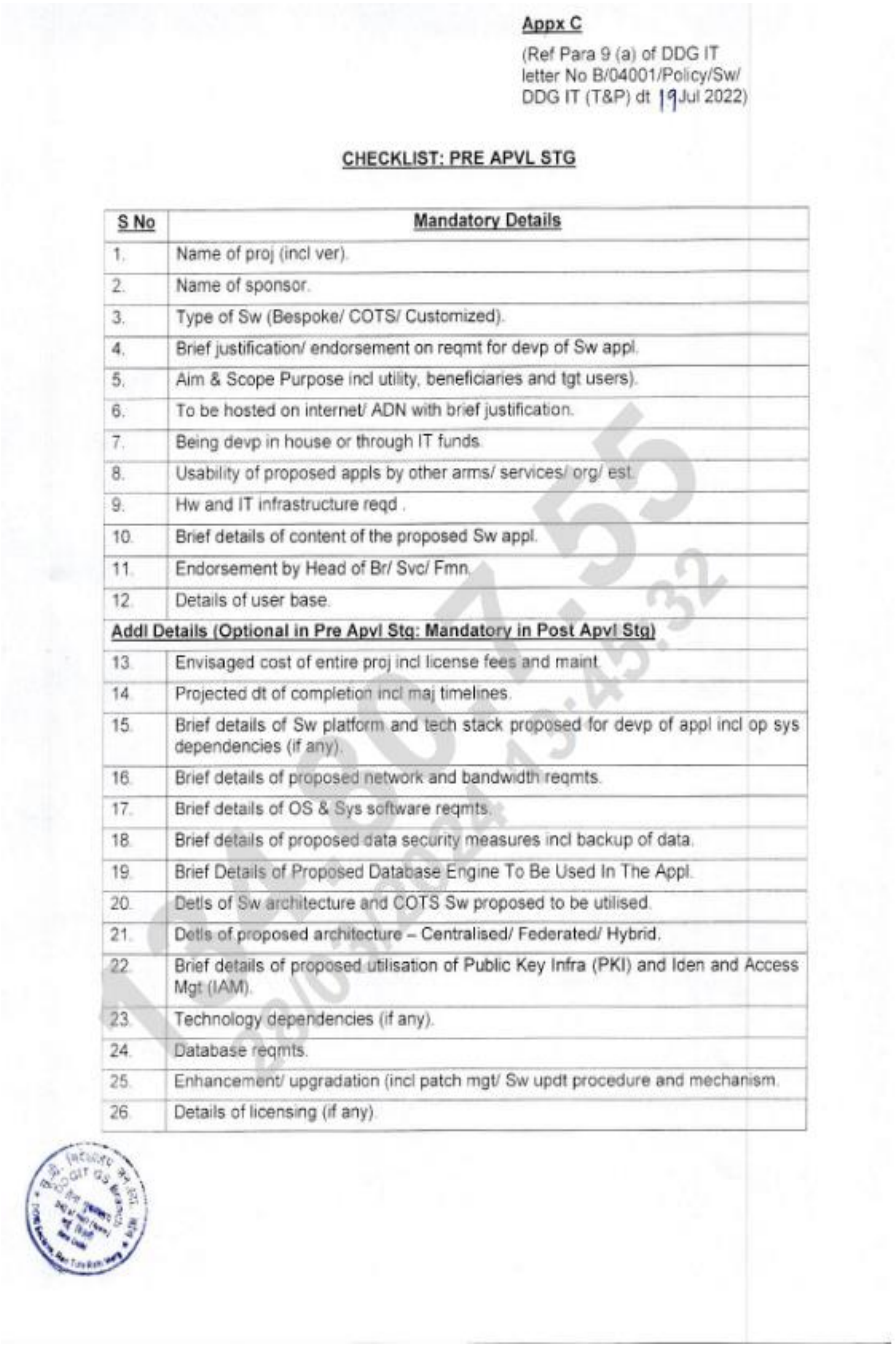
- Coord with AHCC for DNS regn and hosting appl on NIC.
- Ensure through ADG PI that link for the Sw appl has been provided in IA web portal.

LAN/ Stand Alone

Sponsor (PDMG) hosts Sw on LAN/ Stand Alone

ADN

Sponsor submits final Sw appl (VDI/ Executable Image) for hosting at AHCC.



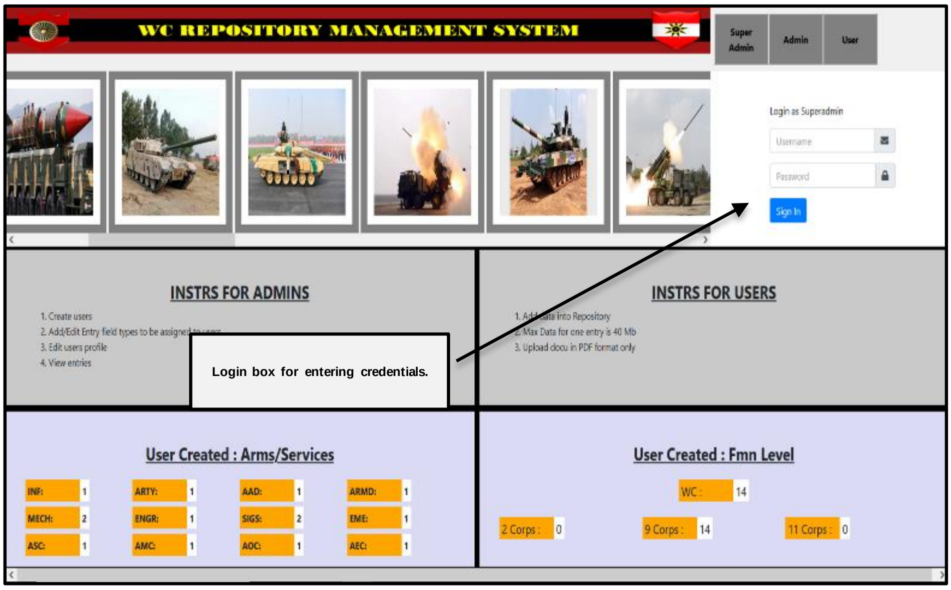
Appx C

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

CHECKLIST: PRE APVL STG

S No	Mandatory Details
1.	Name of proj (incl ver).
2.	Name of sponsor.
3.	Type of Sw (Bespoke/ COTS/ Customized).
4.	Brief justification/ endorsement on reqmt for devp of Sw appl.
5.	Aim & Scope Purpose incl utility, beneficiaries and tgt users).
6.	To be hosted on internet/ ADN with brief justification.
7.	Being devp in house or through IT funds.
8.	Usability of proposed appls by other arms/ services/ org/ est.
9.	Hw and IT infrastructure reqd .
10.	Brief details of content of the proposed Sw appl.
11.	Endorsement by Head of Br/ Svc/ Fmn.
12.	Details of user base.
Addl Details (Optional in Pre Apvl Stg: Mandatory in Post Apvl Stg)	
13.	Envisaged cost of entire proj incl license fees and maint.
14.	Projected dt of completion incl maj timelines.
15.	Brief details of Sw platform and tech stack proposed for devp of appl incl op sys dependencies (if any).
16.	Brief details of proposed network and bandwidth reqmts.
17.	Brief details of OS & Sys software reqmts.
18.	Brief details of proposed data security measures incl backup of data.
19.	Brief Details of Proposed Database Engine To Be Used In The Appl.
20.	Detls of Sw architecture and COTS Sw proposed to be utilised.
21.	Detls of proposed architecture – Centralised/ Federated/ Hybrid.
22.	Brief details of proposed utilisation of Public Key Infra (PKI) and Iden and Access Mgt (IAM).
23.	Technology dependencies (if any).
24.	Database reqmts.
25.	Enhancement/ upgradation (incl patch mgt/ Sw updt procedure and mechanism.
26.	Details of licensing (if any).

INNOVATION NO 1: DATA REPOSITORY MANAGEMENT SYSTEM



Login as Superadmin

INSTRS FOR ADMINS

1. Create users
2. Add/Edit Entry field types to be assigned to users
3. Edit users profile
4. View entries

INSTRS FOR USERS

1. Add data into Repository
2. Max Data for one entry is 40 Mb
3. Upload docu in PDF format only

Login box for entering credentials.

User Created : Arms/Services

INF: 1 ARTY: 1 AAD: 1 ARMD: 1
MECH: 2 ENGR: 1 SIGS: 2 EME: 1
ASC: 1 AMC: 1 AOC: 1 AEC: 1

User Created : Fmn Level

WC : 14
2 Corps : 0 9 Corps : 14 11 Corps : 0

Welcome Page of Data Repository Management System

1. **Requirement**. Around the World, Armies are leveraging on IT assets to enhance operational effectiveness and logistical efficiency. Recognizing the need for a comprehensive, real time dataset of both own and adversary information, 9 Corps Signal Regiment was tasked with developing a Graphical User Interface based Database Management System. This system allows stake holders to upload critical data regarding the capabilities and resources of both own and adversary forces, creating extensive data libraries. Developed in-house, this system is currently in use with HQ 9 Corps for formulation of automated libraries from all Arms / Services.

2. **Equipment Affected**. Data Repository Management System works on server / client architecture on UADN. The details of equipment are as under:-

(a) **Server End**. High end server with adequate storage space.

(b) **Client End**. PC on UADN.

3. **Category**. IT Application.

4. **Brief Description**. Data Repository Management System is a compiled data library for both own and adversary's equipment/ platform/ weapon system, to be utilized subsequently to augment commanders to plan their operations. Moreover, datasets from various sources/ sensors captured during ISR Exercises/ EWTs/ Operational alerts can be utilized as combined data for planning operations. These datasets (Photo, video, text etc.) are annotated and compiled separately for arms and services for multiple equipment/ weapon/ platform system.

5. **Salient Features**

(a) Real time data entry.

(b) Centralized data repository.

(c) User friendly graphical user interface.

(d) Login for admins (PSOs and HOAs) at HQ Western Comd and other formation HQs for creation of data libraries.

(e) Unique feature of creating fields for classification of database.

(f) Ability to add/ delete info of own and adversary weapon system and equipment.

(g) View tab option for respective arms.

(h) User friendly user interface.

6. **Trials/ Test Carried out**

(a) **Methodology**. The application is hosted by 9 Corps Sig Regt on server/ client network architecture over UADN.

(b) **Conduct**

(i) The application can be accessed on https://134.80.6.151/repository over UADN.

(ii) The user can login on the portal and add data in the form of pictures, videos and documents.

(iii) This data is stored in respective libraries for each user.

7. **Details of Utilization/ Deployment**. The Data Repository Management System is currently in use with HQ 9 Corps for formulation of automated libraries for all Arms/ Services. Subsequently, the application will be deployed in HQ Western Command theatre.

8. **Bill of Material**. In house resources.

9. **Sources of Innovation**. Unit Ideas and Innovation Team.

10. **Approx cost with breakdown**. In house resources.

11. **Date of Innovation**. 22 Feb 2024.

12. **Contact Details**:-

(a)	Name of the Innovator(s)	-	Maj Abhishek Puri Capt Angad Sareen
(b)	Name of Unit & Formation	-	9 Corps Sig Regt HQ 9 Corps
(c)	Unit Address	-	9 Corps Sig Regt PIN- 916909 C/o 56 APO
(d)	Tele No – Mob / Official	-	4-2009-2511 8988044055

BRIEF DESCRIPTION: DATA REPOSITORY MANAGEMENT SYSTEM

INTRODUCTION

1. Data Repository Management System is a specialized software solution designed to efficiently store, organize and manage large volumes of op sensitive data from all Arms/ Services of HQ Western Comd. It serves as a centralized hub where data from various sources can be collated, catalogued and analysed securely. This system facilitates data integration, ensures data quality and provides tools for data retrieval and analysis.

2. By centralizing data storage and management processes, Data Repository Management System enhances data accessibility, supports decision making and ensures compliance with regulatory requirements. It plays a critical role in data driven environments, which will enable our organization to leverage our data assets effectively.

REQUIREMENT

3. Globally, IT Applications are increasingly being used by Armies to enhance operational effectiveness and logistics efficiency. Data such as photos, videos, technical characteristics, descriptions of own and adversary's equipment/ platform/ weapon systems will be utilized for subsequently augment commanders to plan their operations. Moreover, data captured from various sources/ sensors captured during ISR Exercises/ EWTs/ Operational Alerts can be utilized as combat data for specific surveillance.

4. Recognizing the need for the comprehensive, real time data set of both own and adversary information, 9 Corps Signal Regiment developed a Graphical User Interface based Database Management System.

5. This system allows stakeholders to upload data regarding the capabilities and resources of both own and adversary forces, creating extensive data libraries.

6. Developed in-house, this system is currently in use with the HQ 9 Corps for formulation of automated libraries from all Arms / Services.

DESCRIPTION

7. Data Repository Management System is a comprehensive frame work implemented using a server/ client based architecture where the server end requires a dedicated server and the user end requires a PC connected over UADN.

8. Developed using PHP as the programming language and Oracle as the database, the Data Repository Management System encompasses a range of tools and processors that support data storage, integrity, security and accessibility. It includes features such as data indexing, backup and recovery mechanism, data integration from various sources and user access controls.

SALIENT FEATURES

9. The salient features of Data Repository Management System are as under:-

(a) **Centralized Data Storage**. Provides a single, centralized location for storing data from various sources, simplifying data management and ensuring consistency.

(b) **Data Accuracy and Security**. Ensures data accuracy and protects against unauthorized access through UADN security measures, user access controls and regular backups.

(c) **Advanced Indexing and Querying**. Offers advanced indexing and querying capabilities, enabling users to quickly and efficiently retrieve and analyse data, supporting informed decision making.

(d) **Data Integration**. Facilitates the integration of the data from the different systems and sources, enabling comprehensive analysis and reporting.

(e) **Admin Features**. Offers a robust login feature for admin granting them the authority to create and manage libraries within the system. Through a secure admin portal, administrators can establish new libraries, configure new library setting and organized data into structured categories.

(f) **Customizable Fields**. Allows users to create customized fields for the classification of data based records, tailoring the database structure to meet diverse needs.

(g) **Sophisticated Tabbed Interface**. Includes a sophisticated tabbed interface that allows users from all Arms / Services to view and manage data for their respective categories.

(h) **User Friendly Interface**. Design to streamline interactions and simplify data management tasks with an intuitive design. Offers easy navigation through dashboards, clear menu options and straightforward data entry forms.