I/109433/2024

SOP ON WHITELISTING OF APPL SOFTWARE IN IA

Ref: -

(a) Minutes of Mtg: Cyber Security Forum-2018 issued vide MO-12 letter No A/12100/CSF/MO-12 dt 10 Aug 2018.

(b) IA Website Hosting Policy (ADN/ Exclusive LAN/ Internet) issued vide DG Sigs letter No B/46850/IT/Policy/Sigs7(a) dt 09 Oct 2019.

(c) SOP on Hosting of IA Websites/ Web Appls/ Mob Appls on National Informatics Centre (NIC) Server issued vide DG Sigs letter No B/46850/IT/Sigs 7(a)/Policy dt 17 Feb 2020.

(d) Minutes of Mtg: Cyber Security Forum-2020 issued vide MO-12 letter No B/51153/ArCyGp/CSF/T-3 dt 20 Nov 2020.

(e) Policy on re-vetting of Sw appls issued vide DG MO (MO-12) letter No A/12108/Vetting/MO 12 dt 04 Dec 2020.

(f) IA Auto Committees formed vide DCOAS (IS&C) Sectt letter No 57926/ICT/DCOAS (IS&C) Sectt/IS dt 07 Sep 21.

(g) Whitelisting of Appl Sw in IA letter issued vide DGMO/ MO-12 letter No A/12108/Vetting/MO-12 dt 08 Oct 21 & even no dt 09 Mar 2022.

(h) SOP on Whitelisting of Appl Software (SW) In IA issued by DDGIT vide B/04001/Policy/Whitelisting SOP/DDGIT (T&P) dt 19 Jul 2022.

(j) Army Cyber Security Policy- 2023 (Uploaded on ADN).

(k) Advisory on Single Window Clearance Initiative (User Driven Interactive Vetting) issued vide ACG letter ref B/51106/ArCyGp/T-3/T&E/Adv1 dt 24 Aug 2023.

(l) Internet Governing Policy for IA issued vide DG MO (MO-10) letter No A/90222/MO-10/91 dt 08 Jan 2024.

INTRO

1. The world today is witnessing profound increase in Digital footprint and proliferation of Info Tech (IT). All orgs are generating enormous amt of data as also devp Sw appls to utilise this data for enhancing efficiency and productivity of the org. The fd of IT Sw devp being a dynamic subject, regular and frequent tech updt of Hardware and related Sw devp is reqd. 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 by 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 judicious util of devp efforts and resources so as to benefit a larger user base, there is an inescapable need for all Sw appls dply over IT assets proc for use by IA, irrespective of source and funding, to be scrutinised by central agency with wider visibility and understanding of the scope for pan-Army utility and dply.

AIM

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

SCOPE

4. DGIS will be the nodal agency for whitelisting of all Info Sys projs and Sw appls incl COTS for IA. DG Sigs will be the nodal agency for whitelisting of all software/ appls incl COTS for central services incl nw mgt, comn and nw security wrt ADN. This SOP has been formulated to provide a framework for whitelisting of Info Sys projs and Sw appls (incl web appl, mob friendly web appl, Server Client Model appl, Standalone Desktop appl, COTS Sw appl etc) to be dply over standalone/ exclusive LAN, ADN or Internet which have been devp in-house by IA or by Govt agencies as part of MoU or Be-spoke devp or devp/proc through industry from any budget head and dply over IT assets proc for use by IA, irrespective of source and funding.

5. The Cyber Security Forum-2018, has divided the roles of DGIS and DG Sigs and has designated them as the nodal agencies for whitelisting of web appls and websites respectively. Accordingly, DG Sigs has promulgated SOPs on website hosting on Private Nw, ADN and Internet.

6. This SOP elucidates the procedure to be followed for obtaining IPA for all types of Info Sys projs and Sw appls, as well as the procedure for whitelisting of the same. The SOP is laid down in the following parts: –

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

(b) **PART II** Procedure for Whitelisting of Sw Devp In-House/ By Outsourcing to Govt Agencies (No Expdr).

(c) **PART III** Procedure for Whitelisting of Sw devp through Trade (Fin Expdr).

(d) **PART IV** COTS Sw Appls.

(e) **PART V** Guidelines for development of Sw.

(f) **PART VI** Timelines to be followed

(g) **PART VII** Salient aspects.

(h) **PART VIII** Life Cycle Sp of Appl Devp by Sponsor Agencies.

PART I: GEN ASPECTS

7. **Nodal Agency**. DDG IT on behalf of DG IS will be the nodal agency for processing all cases for obtaining IPA through IA Auto Committees. DG Sigs will be the nodal agency for whitelisting of all software / appls incl COTS for central services incl nw mgt, comn and nw security wrt ADN. Sigs-7 on behalf of DG Digs will process all Sw/ appls incl COTS, for comn and nw mgt incl Sw for centralised services on ADN and ADN security for obtaining endorsement by DGMO / MO-10 and by DGMO/ MO-12 respectively. Further, whitelisting

of Sw appls for whom IPA is accorded, less the ones to be whitelisted by DG Sigs (software/ appls (incl COTS) for central services incl nw mgt, comn and nw security wrt ADN) will be processed through DDG IT. Mov of **SoC along with all sp docus duly endorsed by Head of Branch/ Svc/ Fmn**, from sponsors to stakeholders and vice versa, will be through DDG IT. DDG IT will monitor progress of all cases and maint updated status of whitelisting of various Sw appls. The status report, repository of all whitelisted software and list of whitelisted Sw appls whose certificate is no longer valid will be updated on DG IS website regularly by DDG IT. Post dply & stab of PAW (Portal for Appl Whitelisting) the monitoring of the progress shall be done through the ibid appl.

8. **Whitelisting of Sw Appls for Central Services incl Nw Mgt, Comn and Nw Security wrt ADN**. All Sw / appls incl COTS, for comn and nw mgt incl Sw for centralised services and ADN and ADN security will be whitelisted by DG Sigs, post endorsement by DGMO / MO-10 and by DGMO / MO-12 respectively. Bespoke appls devp for the purpose however, would require to be security vetted by ACG, prior to dply.

9. **Ownership**.

(a) Any Sw appl planned to be devp by any Fmn/ Est shall be treated as their product and its ownership shall be of the respective Fmn/ Est, incl database security and risk mgt aspects.

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

(c) Head of the fmn/ unit sponsoring the Sw appl will certify that devp of appl has been done in conformation with policies on the subject and that VDI has been prepared as per instructions in vogue.

10. **Endorsement for Necessity of Sw Devp**. In order to minimise duplication of efforts, approval of respective Head of Dte/ Branch in case of IHQ of MoD (Army) and GOC-in-C (through GS (Sys) Branch) in case of fmn/ unit will be obtained by the sponsor. The sanctioning auth may verify the necessity of effort as also examine whether any similar proposal is already in use or under devp.

(a) 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***.

(b) 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.

(c) **Sw Appls to be Hosted on Internet**. All official Sw appls devp to be hosted on Internet will have links on IA web portal i.e. www.indianarmy.nic.in maint by ADG Strat Comn.

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

(e) A presentation by the developer/ sponsor agency on fn necessity, proposed architecture and proposed data mgt will be given to Auto Committee for obtaining IPA.

(g) Sponsor will work out the estimated Hw reqmts incl memory, storage and processing capb in order to ensure avbl of resources at CDC/ RDC and place the same on file before obtaining IPA, which will be eval during provn of resources by AHCC for judicial util.

(h) **Op Info Sys (OIS) Appls**. Considering the sensitivity of data handled by OIS appls, 'Two Factor Auth' to be mandatorily impl.

(j) All Internet based appls will be devp as mob handset friendly web appls only. No smartphone/ mob appl (android or iOS) will be devp. However, mob appl for 'SAMBHAV' may be proposed in consultation with DG Sigs (STEAG).

11. **Format for fwd of new Sw Proj Proposals**. The proposal of a new Sw proj is to be fwd by sponsor agency with all details as mentioned in Para 20 of the SOP for 'In Principle Approval' of competent Auto Committee. Sponsor is reqd to fwd a Statement of Case (SoC) as per the format in DPM along with detls as per **Appx C** to this SOP. In addition, following details are recom to be incl in the proposal: -

(a) **Problem Statement**. As amplification of 'Brief justification/ endorsement on reqmt for devp of Sw appl' mentioned at S No. 4 of Appx C, it is recom that the felt need of the Sw appl be brought out in the problem statement.

(b) **Flow of Data and Structure**. The dply scenario is reqd to be brought out by the sponsor in S No 6 of Appx C to the SOP. The sponsor must ref to 'Consolidate Data Dictionary & SSOT: Indian Army' published by DGIS and make a list of data eles required from other SSOT appls and list of data eles for which he shall be the SSOT. Additionally, sponsor must bring out how the data is intended to be collected, stored and disseminated by the appl.

(c) **User Base**. 'Details of User Base' mentioned at S No. 12 of Appx C be amplified to list out the intended user base of the Sw appl.

(d) **Roles of the Users**. In addition to the intended user base, sponsor should indicate the role of each of these users, for e.g. 'Data Entry Operator', 'Approver' etc.

(e) **Procurement Committee (PC)**. The sponsor should nominate PC at this stg who will vet the proposal and monitor various devp stgs of the SW appl. Proposals recd without the details of PC (which in turn may be made PMG in post apvl stg) will not be considered by Auto Committee.

(f) **Scalability**. The capb of SW appl to scale up from the proposed dply scenario to a larger user base and a larger Nw should be clearly brought out by the sponsor.

(g) **Resources reqd for Devp**. In order to ascertain the resources that will be committed for the devp it is pertinent that sponsor brings out the envisaged quantum of resources reqd for devp of the prosed SW appl.

(h) **Devp Team/ PDMG**. It is proposed that the SW devp be done centrally at ASDC / DG IS as per the DevSecOps model of SW appl devp. Accordingly, all the various components involved in devp, vetting and usage of the appl need to be

I/109433/2024

incorporated at all stgs of devp. A proposed breakup of the devp team/ PDMG is att at **Appx D**.

12. **Automation Committee**. DDG IT will ref cases received as above to **Steering Automation Committee (SAC)** for grant of IPA and approval of data tfr through API. *MI-11 rep will be reqd to attend SAC mtg as a Spl Invitee, if the proposed Sw appl is intended to be dply on Internet.* **IPA** will be accorded by competent Automation Committee based on the estimated cost of the proposal as per following parameters: –

(a) **Steering Automation Committee (SAC)**. Upto ₹ 50 Lakhs.

(b) **Oversight Automation Committee (OAC)**. Above ₹ 50 Lakhs and below ₹ 5 Crs.

(c) **Empowered Automation Committee (EAC)**. Above ₹ 5 Crs.

Responsibilities & Charter of Duties

13. **EAC**

(a) **Responsibilities**

(i) To act as Strat-level apvl committee for all pan IA auto proj.

(ii) Monitor and eval tech infusion in IA through auto. Sponsor to ensure that the case for processing of waiver is endorsed by MO Dte before presenting the Case in SAC and EAC.

(iii) Approve 'Way Forward' in case of issues that crop up during impl of all pan Army appls / auto projs.

(iv) Approve HR reqmts (if any) wrt any pan Army appls/ auto projs.

(b) **Charter of Duties**

(i) To conceptualise digital army vision of IA and provide broad guidelines for enhancing the awareness and accountability of stakeholders at strat and op level.

(ii) To approve structures, procedures and policies reqd for impl of Pan IA projs above **₹ 5 Cr** as proposed by OAC/ SAC.

(iii) To approve fwg for impl of Pan IA auto projs :-

(aa) Mid-course amdts.

(ab) Ratify changes in governance bodies.

(ac) Approve 'Way Ahead' for tech absorption.

(ad) Foreclosure of projs apvd earlier.

(ae) Alternate apchs to meet sch/ overcome technical challenges.

(iv) To ratify MoUs/ SLAs with other agencies as per recom of OAC/SAC.

(v) To ratify all HR reqmts / trg / maint sp incl life cycle mgt reqmts of Pan IA auto proj as proposed by OAC.

(vi) To monitor fwg aspects wrt auto in IA:-

(aa) Info Sys / Digital Army Reqmts.

(ab) Maj milestones to be achieved.

(ac) Auth remedial actions / policy waivers.

(vii) To process policy matters requiring reviewing for apvl of VCOAS.

(viii) Dispute redressal betn Dtes/Cross-verticals/Comds wrt auto issues incl waivers on security related disputes.

14. **OAC**

(a) **Responsibilities**

(i) To act as a higher-level monitoring committee for all Pan IA auto projs.

(ii) Review decisions undertaken by the Steering Automation Committee (SAC) and approve 'Waiver' to existing policies as recom by SAC. Sponsor to ensure that the case for processing of waiver is endorsed by MO Dte before presenting the Case in SAC and EAC.

(iii) Monitor devp process and dply of all pan Army appls / auto projs on ADN.

(iv) Monitor expeditious impl of decisions given by EAC.

(b) **Charter of Duties**

(i) To review the fwg for all Pan IA Auto Projs :-

(aa) Decisions of SAC (incl apvl of 'Waiver') and disposal of auto proj of value above **₹ 50 lacs** upto **₹ 5 Crs**, under intimation to EAC.

(ab) Physical prog of appl / projs apvd earlier wrt compliance of milestones as laid down for its completion and/or recom security related waivers for consideration of EAC.

(ac) Exam expdr for future/apvd projs.

(ad) Policies / procedures / structures.

(ii) To oversee impl wrt fwg :-

(aa) Iden of tech & adm impediments, incl IFA and ACG obsns.

(ab) Exam ADN integration issues.

(ac) Prog HR reqmts/ trg/maint incl lifecycle mgt.

(iii) To monitor fwg aspects of Pan IA Auto projs :-

(aa) Fin prog.

(ab) Commitments made by DAs and slippages there-off.

(ac) Impl strat.

(iv) Subsume functions and resp of the Data Governance Bd.

(v) To ensure fulfilment of contractual obligations at pre-determined stgs.

15. **SAC**

(a) **Responsibilities**

(i) To act as a functional level Steering Committee for all IA Auto projs.

(ii) Facilitate, provide guidance and process for apvl the architecture for all Pan Army appl/ auto projs.

(iii) Recom any 'Waiver' to existing policies in order to facilitate the devp and dply of appls / projs on the ADN.

(iv) Monitor devp, facilitate trials & dply on ADN of all Pan IA Appls/ Auto projs

(b) **Charter of duties**

(i) Take detl bfg on pan IA appl / auto proj by respective appl / proj developers / Proj Devp Mgt Gp (PDMG) for all auto projs. SAC will deliberate and disposal of all cases of value upto **₹ 50 Lacs** at their level by keeping OAC informed. The projs above **₹ 50 Lakhs** will be proposed to OAC for deliberations and apvls. The appl/ proj developers /PDMG may be reqd to undertake the bfg through Video Conf/in person.

(ii) To steer impl of Pan IA appl in terms of policy guidelines, budgetary allocation and timeframes.

(iii) To monitor the fwg for all Pan IA appls / auto projs :-

(aa) Timelines for proj.

(ab) Timely devp, trials, dply of ppl/ auto proj as per QRs/contract.

(ac) User trials and trg.

(iv) To propose fwg for consideration of EAC/ OAC: -

(aa) Waiver to any existing policies.

(ab) Guidance wrt aspects of comn, integ and security.

(ac) HR reqmts / main tsp incl life cycle mgt.

(ad) MoUs/agreements reqd to be signed with other Govt org/ agencies / pvt agencies wrt auto in IA.

(v) To aid in exec of all Pan IA appl wrt:-

(aa) 'Go-Ahead' to undertake devp of appls, dply on ADN, validation of cyber security, post apvl by OAC.

(ab) Interact with user Fmns, Line Dtes, Sister Services, MoD and Devp Agencies.

(ac) Facilitate and provide guidance wrt comn, integ and security aspect related to appl/proj devp.

(vi) To process the impl of all waivers / contracts with existing guidelines/ policies once apvd by appropriate auth.

16. On receipt of IPA or simultaneously, the proposal along with projected cash outlay may be projected to respective High-Level Budget Holder (HLBH) by the sponsor agency for inclusion in IT PPP. The case will be progressed for AoN by respective CFA only after listing it in IT PPP. If conditional IPA is accorded by Automation Committee then sponsor must ensure that all conditions specified by the committee are met before vetting and dply of the Sw appl.

17. **Resp of Stake Holders**

(a) **DDG IT**

(i) To recom to SAC the Sw appl proposal from dupl and utility pt of view. Obtain comments of associated Dte/ Branch at IHQ of MoD (Army), if deemed necessary by Auto Committee.

(ii) Process the case file for clearance by stake-holders post devp of the Sw appl.

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

(i) Platform being used.

(ii) Database proposed to be used.

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

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

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

(c) **DG Sigs/ AHCC**. To analyse the Sw appl proposal with respect to the fwg: –

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

(ii) Integration of the appl with Iden and Access Mgt (IAM) framework for role-based access as a mandatory pre-requisite.

(iii) For integration with Public Key Infra (PKI), for added security if the proposal so necessitates.

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

(v) The sponsor will conform to the checklist for Layout & Arch Vetting att to these instrs.

(d) **DG MO (IW) / ACG**. Vetting of case file of the proposed appl from cyber security perspective. The sponsor should confirm to the best security practices needed to be incorporated in the appl as listed in the user reqmt docu hosted on CERT-Army website on ADN.

(e) The sponsor agency will confirm adherence to the checklist prepared based on instructions/ guidelines/ policies promulgated by various stake holders and compiled and att at Appx C to this SOP.

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

(g) Sponsor agency will proceed with devp of Sw appl post grant of IPA.

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

18. This procedure is only applicable for devp of Info Sys projs or Sw appls wherein no cost to exchequer is envisaged. All in-house devp by enthusiastic coders of IA or devp by Govt agencies/ PSUs on NCNC basis or devp by agencies as part of MoU will follow this procedure.

19. The procedure for whitelisting of proposals will have following two stgs, flowchart for which is given at **Appx E & F** to this SOP: –

(a) Pre devp stg.

(b) Post devp stg.

Pre Devp Stg.

20. This stg entails **In Principle Apvl** (IPA) by competent Auto Committee to the sponsor agency as a ‘go ahead’ and to further process the case file. In order to ensure that all members of Auto Committee are adequately prepared to discuss the case and to cut down the time taken for grant of IPA, sponsor agency will fwd copy of case file to all stakeholders viz DG IS (DDGIT and ASDC), DG Sigs (AHCC) & DG MO (ACG) through ASIGMA/e-Office or in the form of physical files.

21. **Processing of Case File**. The proposal will be duly endorsed by Head of Dte/ Branch in case of IHQ of MoD (Army) and GOC-in-C in case of fmn/ unit. Sponsor agency will fwd case file through HQ Comd GS (Sys) Branch, along with fwg docus to all stakeholders: –

(a) S of C as per DPM - 2009 and amdts thereto, duly endorsed by competent auth.

(b) **Checklist**. Completed checklist with details mentioned as mentioned in **Appx C** be included in case file for processing.

I/109433/2024

22. **Proj Devp & Mgt Gp (PDMG)** A PDMG will be formed under the aegis of the sponsor agency to ensure the fwg: –

(a) Est the ownership of Sw.

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

(c) Reg monitoring of the prog of proj and fwd regular feedback to DDG IT regarding progress of proj.

(d) In case of change in scope of proj or reqmt of addl funding from DDG IT as the HLBH, the same will be intimated to DG IS after getting the revised proposal duly endorsed by the competent auth.

(e) Mgt of the Sw appl throughout its entire lifecycle (details at Para 39 below).

(f) A rep of 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.

23. 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.

24. All stakeholders (as under) shall analyse the case-file based on the inputs fwd by sponsor before the matter is discussed in Automation Committee.

(a) **Sw Appls to be Hosted on ADN/ LAN/ Internet**. DDG IT, ASDC, AHCC & ACG.

(b) **Sw Appls to be Hosted on Stand Alone PC**. DDG IT, ASDC & ACG.

25. **Sw Appls to be Hosted on Internet**. Fwg details, **in addn to a/m**, will also be incl in the case file: -

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

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

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

(d) Single pt contact for Sw appl.

(e) MI clearance for content proposed to be hosted/ collected through these Sw appls may be obtained prior to devp.

Post Devp Stg.

26. Once the Sw appl has been devp by the sponsor agency, the flowchart as per Appx F to this SOP shall be followed. The sequence of actions will be as under: –

(a) Sponsor agency to upload final Sw Appl (VDI/ Executable Image) in the test envt at **ACG** with cont access for testing and validation by DG Sigs and ACG. Only appl to be hosted on ADN /OIS applications / applications handling data of security cl

I/109433/2024

CONFIDENTIAL or higher shall be security vetted by ACG. Applications to be hosted on Internet shall be security vetted by a civ CERT-In Empanelled auditor.

(i) **ACG**. Will host the devp Sw appl in test envt on ADN with cont access to AHCC and developer. AHCC will undertake the architectural vetting of the appl (elaborated in succeeding Para) and post architectural vetting clearance, cyber security vetting specific to the dply scenario would be undertaken by ACG. Pre-requisites for same are att as **Appx H**. To assist testing team in understanding appl workflow and architecture, a pstn shall be conducted by the sponsor. Cyber security vetting at ACG to be undertaken in two phs for ADN appls i.e Lab Test Ph and Remote Test Ph (Flowchart of the same is att as **Appx J**). Post Lab Test clearance sponsor to liaise with AHCC/DG Sigs for IAM integration to facilitate Remote Test.

(ii) **AHCC**. Will remotely access and validate the dply architecture, authentication, security overlays and BW reqmts of Sw appl to be hosted on ADN, as apvd initially during approval 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.

(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 an external CERT-In Empanelled vendor by the sponsor agency. The cost of the same will have to be incl in the overall cost of the proj.

(iv) Sponsor agency to submit final Sw appl (VDI/ Executable Image duly vetted by AHCC & ACG) to DG IS (DDG IT) along with copy of Cert In empanelled auditor clearance (if applicable), MI-11, AHCC and ACG clearances.

(v) Sponsor agency to coord with MI-11 under intimation to DDGIT for content vetting of Sw appl by them.

(vi) A copy of VDI of the final vetted Sw appl along with checksum will be submitted to DDGIT who will maint the digital repository of Sw appl devp by IA. Provisions for extension of validity shall be as per para 37 below.

(vii) On submission of all clearances for the sw appl and **VDI of the final vetted Sw appl (along with checksum)** to DDGIT, the Whitelist Certificate shall be issued to the sponsor agency under intimation to ACG and AHCC.

(viii) AHCC will dply the appl in Data centre with access cont administration right given to sponsor agency through IAM.

(b) **Hosting of Sw Appl**. Sw appl will be hosted as follows **only after it has been Whitelisted by DDGIT/ DG Sigs (as applicable)**: –

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

(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.

I/109433/2024

PART III: PROCEDURE FOR WHITELISTING OF SW DEVP THROUGH TRADE

27. This procedure is applicable to devp of all Info Sys projs and Sw appls in which expdr is envisaged. All proposals intended to be devp by trade/ industry or vendor or freelance devp or PSUs on payment and whose RFP would be prepared as part of the proposal is covered in this category.

28. This procedure for whitelisting of Sw appls wherein cost is involved is divided into three stgs :-

(a) **Pre Devp Stg**. All activities at this stg are same as the one elucidated in Part-II above. Details mentioned as per 'Appx C' will be fwd for processing in this stg.

(b) **RFP Vetting Stg**. Elaborated below at para 29.

(c) **Post Devp Stg**. All activities at this stg are same as the one elucidated in Part-II above. The sponsor must ensure that the Sw appl devp conforms to the RFP vetted by the stake holders so that security and content vetting is carried out in a time bound manner.

29. **RFP Vetting stg**. Post grant of the IPA, the RFP shall be fwd by sponsor for vetting by the stakeholders. The supply order for devp of Sw appl shall be awarded to the selected developer to make the Sw that meets the QR mentioned in RFP and by following the devp mechanism elucidated in the RFP. Accordingly, it is pertinent that all agencies involved in testing and vetting of Sw appl post devp do *apriori* vetting of the proposed RFP. The RFP vetting broadly constitutes of fwg two aspects: -

(a) **Fin/ Adm Vetting**. Fin/ Adm vetting is to ensure that RFP conforms to the proc policy laid down by MoD, Govt of India. Fin/ Adm vetting of RFP shall be done by CFA rep as per the estimated cost of the proposal.

(a) **Tech Vetting**. Tech vetting shall be done by the tech stakeholders viz DG IS (ASDC), DG Sigs (AHCC) & DGMO (ACG for pan Army proj and respective CCOSWs for proj upto Comd level). The responsibilities of all concerned stakeholders have already been discussed at para 13 above. The sponsor shall send the RFP to all the stakeholders **concurrently**, under intimation to DDG IT, to expedite the vetting. Post vetting of RFP, the sponsor shall proceed with proc procedure and devp of Sw appl after incorporating the inputs recd from stakeholders. The flowchart for RFP vetting is given at **Appx G** to this SOP.

PART IV: COTS SW APPLS

30. 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.	(i) Sponsor must iden & select the specific COTS Sw through a BOO as per para 30 below. (ii) Case for IPA to proc the identified COTS Sw appl will be fwd to DDG IT for consideration of Auto Committee. (iii) On grant of IPA the proc will be completed and VDI (if source code is avbl) will be fwd to DDG IT.	(i) **IPA so accorded 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) **IPA so accorded 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.		

31. **Selection of COTS Sw**. The sponsor should follow the proc procedure as laid down to identify the COTS Sw. Alternatively, a Bd of qualified offrs will be convened who will assess the identified COTS Sw appl for conformation to following parameters: –

(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) **Data 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 atching the client's desired Protection Profiles (PPs) with the Security Targets (STs) provided by the vendors

32. Any COTS appl whitelisted by DDGIT will be deemed as whitelisted for use pan IA in the similar dply scenario i.e. if a COTS appl is whitelisted for pvt LAN, then any other Dte/ fmn may use the pvt LAN only. However, whitelist cert will **NOT** be considered as auth for proc and the users will adhere to extant policies for proc through GeM.

PART V : PROCEDURE FOR DEVP OF SW APPLS

33. The nature of Network Centric Projects calls for the use of software consisting of applications and systems deployed over various networks. Software plays a pivotal role in Network Centric Projects, and the quality and performance of the Project as a whole hinges on quality and performance of the software and of the network. Software design is modular, permitting assembly of software systems by integrating a mix of existing and new applications, and ensuring that the end product is capable of integrating with the network.

34. The development of Software for Network Centric Project can be classified into five different phases, viz: -

(a) **Requirement / Specification Phase**. The goal of this phase is to understand and collect the exact requirements of the user and to document them properly. Developer/Supplier will capture the User requirement through detailed interaction with the User and will prepare System Requirement Specification comprising of Software Requirement Specification (SRS), Interface Requirement Specification (IRS) and Hardware Requirement Specification (HRS). These System

specifications will translate into System Requirement Description to include Software Requirement Description (SRD) which will be duly approved by the User. The SRD will be vetted by all stakeholders during the pre-approval stage.

(b) **Design phase**. The goal of this phase is to transform the Software Requirement Specification (SRS), Interface Requirement Specification (IRS), and Hardware Requirement Specification (HRS) into a structure that is suitable for coding and construction. Here, overall software architecture is defined and a document called Software Design Document (SDD) is prepared. In Design, the documents will be prepared by the Vendor/Supplier after detailed interaction with User and approval of the document by the User. The major activities during the Design Evaluation shall be to trace the Requirements to Spec (Hardware Requirement Specification /Software Requirement Specification / Interface Requirement Specification) and the test cases duly for validating the specifications defined by the Firm and/or Developer.

(c) **Testing phase**. Once the software is coded, it is tested for verification and validation purpose. Developer / Supplier in consultation with User (if required) will prepare TVPR (includes TVPR & metric formulation & validation) and Test Cases. However, TVPR & metrics will be vetted by the stake holders and/or IV&V Team during Requirement and Design Evaluation. The Developer/ Supplier SQC and SQA teams shall there after prepare test reports and carry out Component / Module Unit &Integration, and testing for Functional and Acceptance tests on Software. Stake holders shall be undertaking Integrated System Testing after successful integration of the Software and the System. The User may be co-opted during the Acceptance, Installation and Commissioning Tests. The summarized role of the firm and stake holders in this stage shall be as follows: -

(i) **Modules and Unit Testing to be undertaken by the Developer.** Corrective and Preventive Actions taken in case of failure to be shown to the stake holders for Audit & Review.

(ii) **Integration Testing to be carried out by the Developer. T**he reports to be produced to the stake holders for Audit & Review.

(d) **Implementation phase**. After the testing is completed, the software is implemented/deployed and made operational over the actual condition it is made to work for.

(e) **Maintenance phase**. Software maintenance is very broad activity which includes error correction, enhancement of capabilities, and deletion of obsolete capabilities and optimization of the software.

Software Quality Assurance Approach

35. **The Software Quality Assurance**. Chapter 5 of **JSG 1040: 2023** is relevant and approach shall include: -

(a) Review and Audit of processes for Software Development as per SDLC (ISO/ IEC12207) and Quality Model adopted (in accordance to ISO/IEC 25010 or better) for the purpose of adequacy and correctness checks by the stake holders.

I/109433/2024

(b) Stake holders shall witness/ undertake Black Box Testing at System level and may undertake the Grey Box testing only for critical Assemblies/ Modules/ Units/ Sub-assemblies as part of concurrent testing during development.

(c) Undertaking Verification & Validation (V&V) at System Acceptance Level at Integrity level IV in accordance to IEEE 1012.

PART VI: TIMELINES TO BE FOLLOWED

36. **Timelines For Clearances**. Timelines for according clearances at each stg to the Sw appls (in case there are no obsns) is as under: -

S No	Stockholders	Timeline	Remarks
(a)	DDG IT	01 week	(i) The case file pertaining to Dte / Branch of IHQ of MoD (Army) shall be processed on NIC eOffice. Case files received from HQ Comds to be ingested in e-Office by DDGIT and processed on e-Office till such time Comds are onboarded in e-Office. (ii) The Date & Time Stamp of receipt on eOffice shall be start of stipulated timeline. (iii) The case file shall be cleared before the end of stipulated timeline failing which necessary clearance from the stakeholder shall be **deemed to be accorded**.
(b)	ASDC	01 week	
(c)	DG Sigs	02 weeks	User Driven Interactive Vetting
(d)	MI-11	01 week	
(e)	ACG	06 weeks	User Driven Interactive Vetting

PART VII : SALIENT ASPECTS

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

(a) **Validity**

(i) Whitelisting of a Sw appl gtd to a Dte/ fmn is valid for a pd one yr for Sw appls to be hosted on internet and three yr for those on ADN/ LAN/ Stand Alone, subject to no structure/ code change is made to the sub Sw appl in the interim.

(ii) Sponsor agency will process the case for re-whitelisting of Sw appl with DDGIT for fresh vetting in case of any update/ changes/ mod or end of validity of the whitelisted Sw appl. All stake-holders will do the respective vetting post which DDGIT will issue fresh whitelist cert.

(iii) Sponsor agency will commence the action for re-whitelisting of the Sw appl at least 5 months (150 days) prior to expiry of the current whitelisting cert to ensure timely issue of fresh whitelist cert.

(iv) Sponsor agency will regularly interact with stake holders during re-vetting of Sw appl. During vetting process appl will be deemed to be closed if no response is recd from sponsor within three months of raising a query. IPA previously accorded shall be revoked and sponsor will have to obtain all approvals afresh for such cases.

(v) If a Sw appl is recd for re-whitelisting after expiry of the validity pd, waiver for extn of validity of whitelist cert of the Sw appl will **NOT** be granted.

(vi) Whitelist cert is valid for a specific dply scenario and specific cl of data, but is not specific to sponsor. Any change in dply scenario/ cl of the data being handled by the appl, a fresh case for whitelisting will be initiated by the sponsor. Other Dtes/ fmns may use the whitelist cert for the dply scenario and cl of data under intimation to DDG IT.

(vii) Stake holders will ensure that only whitelisted Sw appl are dply as per approved dply scenario and only data of the approved cl is in use in those appls in the IT assets of IA ests/ fmns/ units irrespective of sourcing or funding of the assets.

(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.

38. **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) Sponsor will submit a copy of the final dply version, less source code, of whitelisted Sw appls to DDGIT. 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 VIII: LIFE CYCLE SP OF APPL DEVP BY SPONSOR AGENCIES

39. Sw appls devp by the envt will be cl as **local or pan Army** appls based on utility and usage. IA Auto Committee will designate Sw appls for pan Army dply during the pre-devp stg. The philosophy for lifecycle sp of appls will be as under: –

I/109433/2024

(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. Handing over of the Sw appl incl knowledge, source code and help files to the next incumbent during turnover of reps of PDMG will be ensured by head of the sponsor Dte/ fmn.

(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

40. 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.

41. This SOP supersedes previous SOP on the subject issued by DDGIT vide B/04001/Policy/Whitelisting SOP/DDGIT (T&P) dt 19 Jul 2022.

Signed by Col Suresh Kumar
Date: 28-05-2024 11:00:54

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

(Suresh Kumar)
Col
Offg Brig IT
For DG IS

DDG IT, Dte Gen Info Sys
General Staff Branch
Integrated HQ of MoD (Army)
New Delhi-110010
Date : As in Digital Sign

All Branches/ Dtes of IHQ of MoD (Army)

All HQ Comds & Corps

Copy to: –

VCOAS Sectt - For your info pl.

DCOAS (IS&C) Sectt

I/109433/2024

Appx A

(Ref Para 10 (d) of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

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 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.

(iv) The data elements during DB design should confirm to the Data Dictionary & SSOT promulgated by DGIS.

(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.

(g) **Virtual Machines Reqmts**. Reqmts of VMs, incl memory, storage and processing capb for catering the same in Data Centre.

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

(c) 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.

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

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

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

3. **Layout and architecture vetting**

(a) **Forms Reqd**.

(i) Website / Appl lab test done by ACG.

(ii) Statement of Case recd.

(iii) GIGW certificate.

(iv) DNS registration form.

(v) Watermark certificate.

(vi) SSL registration form.

(vii) MI-11 Certificate.

(b) **Details of VM**.

(i) No of VM.

(ii) No of CPU per VM.

(iii) Storage reqd per VM.

(iv) RAM reqd per VM.

(v) Operating System of Server (license).

(vi) Back up reqmt.

(vii) VID with size (.vmdk/.msi/.ova).

(c) **Development Platform Used**.

(i) Framework used.

(ii) Details of framework used.

(iii) Security configuration of firewall.

(iv) Version of dependencies.

(d) **Security Details**.

(i) TLS version (ver 1.3).

(ii) SSL implementation.

(iii) Bandwidth used.

(e) **Access Control**.

(i) IAM integration.

(ii) Domain Joined.

(iii) DSC token.

(iv) No of user role.

(iv) Ports used / allowed.

(f) **Database Architecture**.

(i) Database used (MS SQL / My SQL/ SQL lite/Maria db/Oracle/Postgres SQL/ Oracle / No SQL.

(ii) Database VM's.

(iii) Wildcard queries (No of query).

(iv) Query optimization (*Query/ Table Query).

4. **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.

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

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

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

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

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

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

(f) 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.

I/109433/2024

(g) 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”.

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

I/109433/2024

Appx B

(Ref Para 10 (d) of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

CERTIFICATE FROM HEAD OF SPONSOR AGENCY

It is certified that: -

1. All laid down policies, procedures and guidelines for Sw appl devp have been adhered to during devp of the Sw appl.
2. The VDI prepared for _____ appl contains latest version of development environment and dependencies.
3. No unwanted links, tabs, redundant codes & modules are present in the source code.
4. No links to any unwanted external websites is present in the source code.
5. Complete functional testing of the appl has been carried out prior fwd the VDI.

Station:

Date :

(Head of Sponsor Agency)

I/109433/2024

Appx C

(Ref Para 11 of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

CHECKLIST TO BE ATT WITH SOC FOR THE PROPOSAL

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 and 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 in the form of Virtual Machines at Data Centre (incl memory, storage and processing capb).	
10.	Brief details of content of the proposed Sw appl.	
11.	Endorsement by Head of Br/ Svc/ Fmn.	
12.	Details of user base.	
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).	

I/109433/2024

S No	Pre Devp-Stage – To be submitted for grant of IPA	Response of Stakeholder
Sigs-7		
1.	**Hardware Reqmt**. To be rationalized by developer with supported load calculation.	
2.	**Bandwidth Reqmt**. No of concurrent users access the appl on ADN to be highlighted, Common user bandwidth to be utilized no dedicated bandwidth to be provided.	
3.	**Encryption**. IACA SSL cert to be incorporated for secure HTTPS connection (TLS 1.3 should be impl).	
4.	**IAM**. Appl developer to design and devp the appls for integ with IAM (SAML 2.0 needs to be followed).	
5.	**Ports**. 443 port to be used for hosting, any addl port reqd should be justified.	
6.	**Software**. Sponsor Dte to provn for licensed OS and other reqd softwares for the appl.	
ACG		
1.	Advisory on Appl Security: Evolving (URD) User Requirement Document (Hosted at ACG Website - Web/Appl Devp - Test & Eval Advisories).	
2.	Impl of Secure Coding Prac in IA : HCL AppScan VS CodeSweep (ACG letter No B/51106/ArCyGp/T-3/T&E dt 04 Aug 23).	
3.	Advisory on Cyber Security Parameters for Websites hosted within ADN (Hosted at ACG Website - Web/Appl Devp - Test & Eval Advisories).	
4.	Guidelines for Indian Govt Websites (GIGW 3.0).	
ASDC		
1.	Platform to be used - check and render advice on Long Term Sp incl the End of Life.	
2.	Database to be used – check and render advice on Long Term Sp incl the End of Life.	
3.	Software architecture and COTS Sw dependencies – native/ webbased/centralized/ decentralized, offline/online mode, Selection criteria of COTS Sw etc.	
4.	Integration reqmt with other Sw (online/ offline) – recommend appls alongwith the requisite formats of exch.	
5.	Usability of Sw by other arms/services/fmns/orgs – advise sponsor fm scalability pt of view.	

I/109433/2024

S No	Post Devp Stage – To be submitted for vetting of Sw appl.	Response of Stakeholder
Sigs-7		
1.	**OS & Software**. (a) OS and softwares used in appl should be activated (licensed) if applicable. (b) The OS and the softwares used should not be outdated. (c) The appl should not use vulnerable scripts and libraries.	
2.	**Hardware Resources**. (a) The hardware resource used by the appl should be justified by the sponsor Dte with valid calculations. (b) Stress testing of the appl is done with the anticipated concurrent users to check the hardware utilization of the appl. (c) A website with up to 1000 concurrent users should not consume more than 8 CPU cores and 16 GB RAM. (d) A relational database server (Mysql/MSsql/Postgres) with 1000 concurrent users should not consume more than 24 CPU and 48 GB RAM. (e) A web appl server with 1000 concurrent users should not consume more than 16 CPU and 32 GB RAM. (f) A Geospatial server (GIS) with 1000 concurrent users should not consume more than 32 CPU and 64 GB RAM.	
3.	**Compliance**. (a) Websites should follow GISW present. (b) All the downloadable data (PDF) should be watermarked. (c) **Links** (i) No broken links to be present. (ii) All the websites / appl linked in the page should be vetted. (iii) Only whitelisted SW (as per ACG guidelines) links to be provided for download. (d) Metatags should be enabled. (e) No direct streaming of Video / Audio.	
4.	**IAM**. (a) IAM integ to be completed (SAML 2.0). (b) Encrypted login and logout to be implemented. (c) User list (usernames in domain) to be on-boarded should be shared with AHCC. (d) Two factor authentications if reqd should be impl with IACA DSC token.	

5.	**Deployment Arch**. (a) Sponsor Dte to give a pstn explaining the entire workflow on the sw appl along with its detailed dply architecture. (b) Sponsor Dte / developer to explain all the intended functionalities and features of the appl. (c) Clarify any ambiguities or discrepancies with the devp team before commencing the vetting process. (d) Strict version control to be adhered during the iterative process of vetting. (e) The appls requiring PKI services, must have inbuilt OCSP and CRL protocols for certificate validation.	
6.	**Performance / Stability Testing**. (a) Appl / Website initial loading on the browser should not be more than 4 MB (screenshot att at Appx A). (b) The max response time for the appl / website should not be more than 5 seconds. (c) The appl should not crash when load tested with anticipated concurrent users.	
7.	**Functional Testing**. (a) Perform testing of each indl function and feature of the web appl. (b) Validate input fields, forms, button navigate and interactive elements. (c) Verify proper data validation, error msgs and expected outcomes.	
8.	**Compatibility Testing**. (a) Should be compatible with older supported versions of browsers (chrome / edge / firefox). (b) Shuld be compatible with different versions of third-party plugins or framework. (c) Regression Testing – Retest previously identified issues after fixes have been implemented. (d) Ensure that fixes have not introduced new problems or unintended side effects.	
9.	**Encryption**. IACA SSL cert to be incorporated for secure HTTPS connection (TLS 1.3 or latest should be impl).	
10.	**Forms Reqd**. GIGW cert, DNS regn form, DGMI (MI-11) content vetting form, Watermarking cert, SSL regn and SRDP regn form are rqd to be submitted to DG Sigs for hosting on ADN.	
ACG		
1.	Advisory on Single Window Clearance Initiative (ACG letter ref B/51106/ArCyGp/T-3/T&E/Adv1 dt 24 Aug 2023).	

I/109433/2024

2.	Advisory on Tech Vetting for Whitelisting of Sw for AND Dply (DG Sigs letter ref B/46850/IT/Sigs 7 (a) dt 03 Mar 2022).	
3.	User Friendly Guidelines for Expediting Vetting if Websites/ Web Appl (Hosted at ACG Website - Web/Appl Devp - Test & Eval Advisories).	
4.	CERT Advisory No 08/2023 on conduct of Vulnerability Analysis of Sw of IA by CERT-IN Empanelled Firms (Hosted at ACG Website - Web/Appl Devp - Test & Eval Advisories).	
5.	Advisory No 12-2016 on Hardening of Web Server, How to make VDI for Web Testing, Web Testing Tool, Patch Mgt and OS (Hosted at ACG Website - Web/Appl Devp - Test & Eval Advisories).	
6.	Further, for the better transparency and user awareness, real-time appl vetting status is hosted on ACG Website (ACG Website - Web/ Appl Devp - Web/Appl Vetting Status).	
7.	CERT Advisory No 13/2023 on API Security.	
DDGIT		
1.	Fwd VDI of final Sw appl.	
2.	Fwd data dictionary of data and meta data.	
3.	Obtain Whitelisting Cert.	

I/109433/2024

Appx D

(Ref Para 11 (h) of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

PROPOSED BREAKUP OF THE DEVP TEAM/ PDMG

S No	Role	Work Content	Responsibility
1.	Program Manager	(i) Continuously manages throughout the program lifecycle. (ii) Plans the overall program and monitors progress. (iii) Manages budget, risks, and issues, and takes corrective actions.	Sponsor
2.	Pipeline Architect	Leads the technical design, development, and evolution of the pipeline.	ASDC
3.	Culture Change Coach	Plans, organizes, coordinates, facilitates, and reports on culture change activities and progress.	Sponsor & Development Agency
4.	PMU	Interacts with the software in the operational environment	Sponsor
5.	End User	Benefits from interacting with the delivered system in production.	User
6.	Software Engineer	(i) Writes code based on requirements. (ii) Tests and delivers programs and sys. (iii) Fixes and improves existing software.	Development Agency
7.	Requirements Engineer	Works with stakeholders (Services PMU) to elicit, understand, analyze, and document requirements for a project.	Sponsor
8.	Test Engineer	(i) Creates and documents test cases. (ii) Performs and docus risk analysis (iii) Codes and runs automated tests. (iv) Determines product quality and release readiness.	Sponsor in consultation with ASDC, Sigs-7 & MO Dte
9.	Operations Engineer	(i) Operates by accessing software on computers (ii) Monitors and manipulates daily system jobs (iii) Starts operations by entering comds (iv) Performs defined tasks per documented instructions/processes	Sponsor & User
10.	Security Engineer	**Security Engineer**. Performs security testing and code review after devp of Complete Software.	ACG

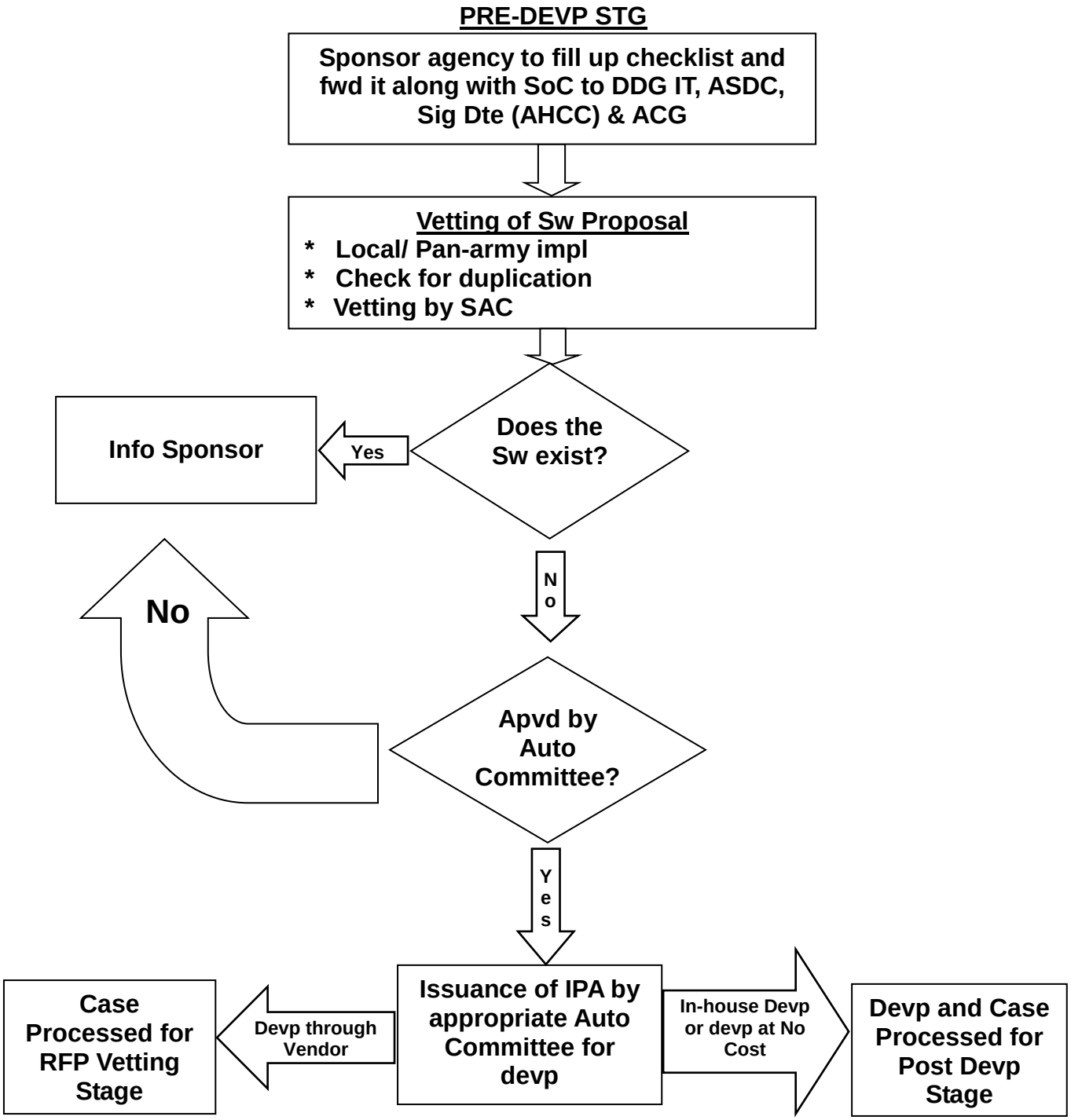
(It is proposed that sponsor should coord with all the stakeholders in the Centralised Sw Devp team and form the DevSecOps team/ PDMG as mentioned at Para 22 of SOP post grant of IPA)

I/109433/2024

Appx E

(Ref Para 19 of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

FLOW CHART: WHITELISTING OF APPL SW IN IA

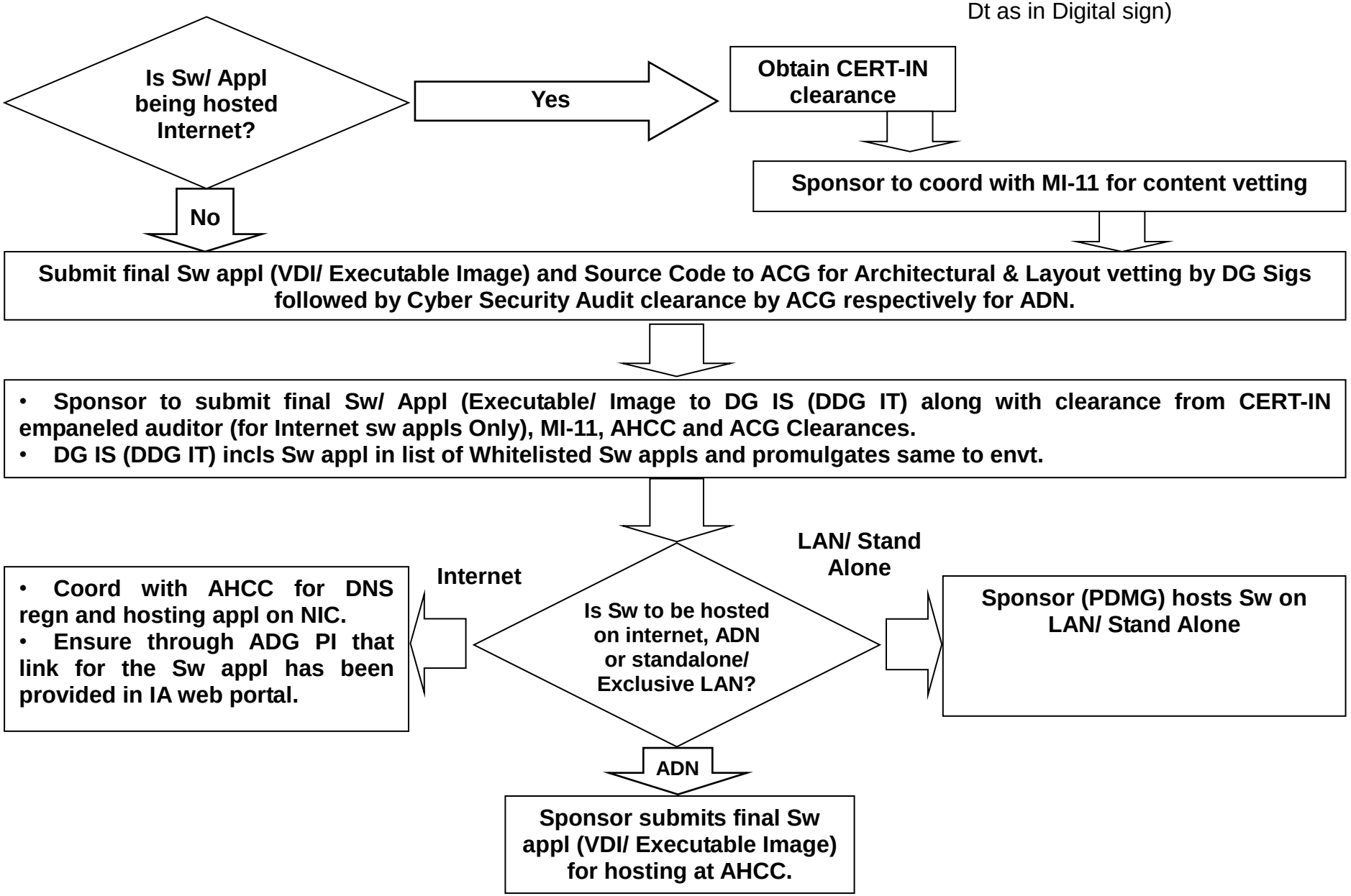


I/109433/2024

Appx F

(Ref Para 19 of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

POST DEVP STG

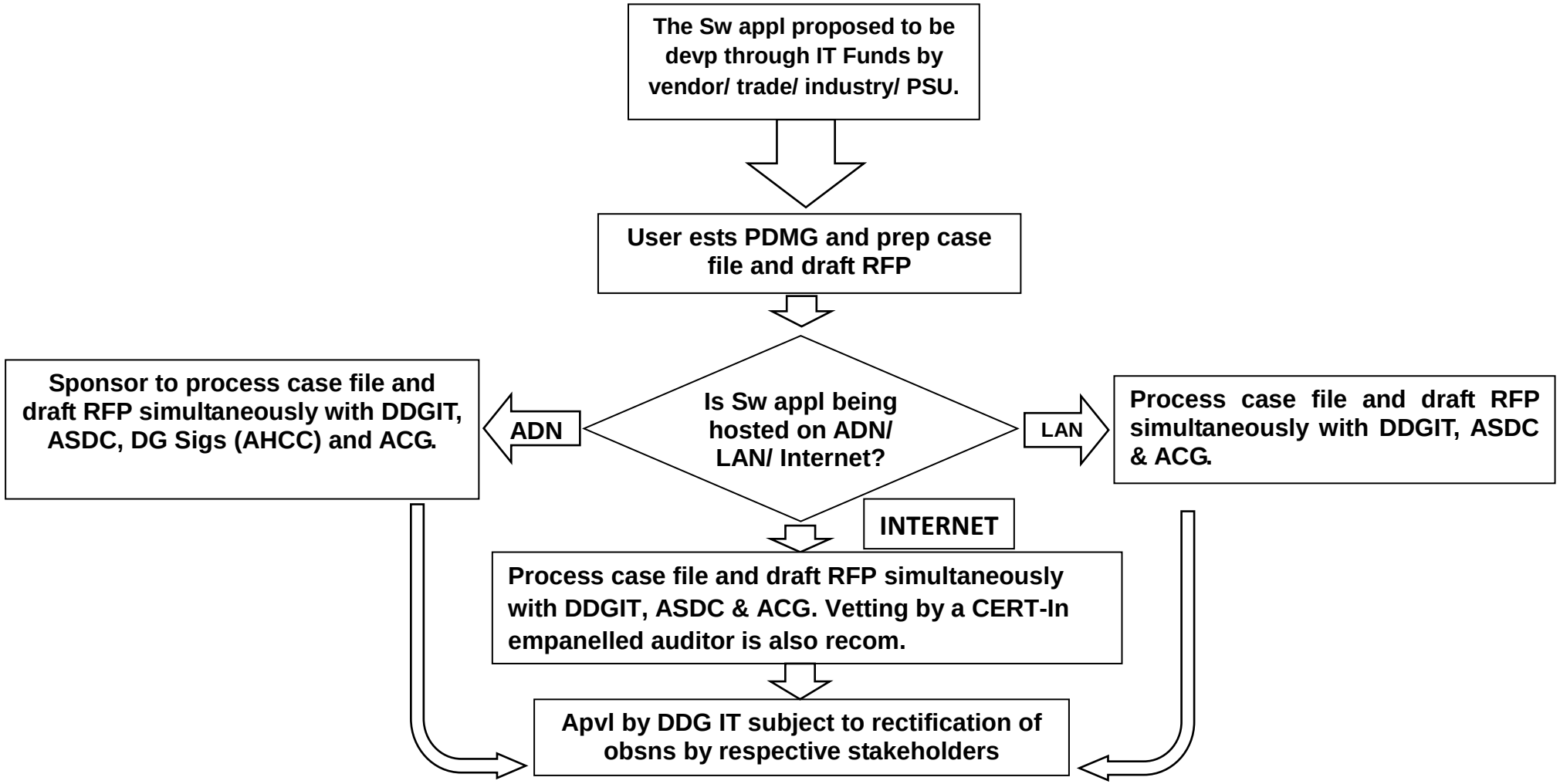


I/109433/2024

Appx G

(Ref Para 29 (b) of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

RFP Vetting Stg



I/109433/2024

Appx H

(Ref Para 26 (a) (i) of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

PRE-REQUISITES FOR UNDERTAKING CYBER SECURITY AUDIT

1. **Websites**.
   - (a) As per approved template.
   - (b) Web Vuln Analysis Tool Scan report with no vulnerabilities.
   - (c) Server OS and other dependencies with min 3 yrs lifecycle sp.
   - (d) Latest dependencies and components.
2. **Web Appls**.
   - (a) IPA by SAC.
   - (b) Appl testbed with source code in Debug mode.
   - (c) Layout and arch vetting clearance (ADN only).
   - (d) CERT-In empanelled auditor audit report with “Safe to Host” (Internet only).
   - (e) Dummy data populated.
   - (f) Detl user trials and functional testing undertaken.
   - (g) Server OS and other dependencies with min 3 yrs lifecycle sp.
   - (h) Credentials of all roles in the appl.
   - (j) Appl code finalised and Code frozen cert by sponsor.

I/109433/2024

Appx J

(Ref Para 26 (a) (i) of DDG IT letter No B/04001 /Policy/Sw/DDG IT (T&P) Dt as in Digital sign)

FLOWCHART OF CYBER SECURITY VETTING AT ACG