

PROPOSAL FOR DEVP OF CYBER SHAKTI SW APPL

1. **Background.** There are almost 621 computers, 52 MFDs and 46 Internet connections held with HQ Southern Comd. The fmns under HQ Southern Comd also hold no of computer assets due to overall influx of IT into IA. Therefore, there is a need to account for all the IT assets at all fmns as well as carry out timely maint and cyber audit thereby mitigating the obsns to maint cyber hygiene.

2. **Need.** Presently all accounting & record is maint manually. Need was felt to devlp an appl to account for all IT assets in terms of maint carried out & cyber record on regular basis. This will maint the record of all IT assets and facilitate timely mitigation of any faults or cyber obsns. This SW appl will be a single platform to maint the cyber hygiene of the fmn. Therefore, an appl to meet above requirement was designed & named as 'Cyber Shakti' to maint the record of all the data related to computers on single platform to avoid duplicacy & transparency to maint the cyber hygiene.

3. **Proposed structure of Cyber Shakti.** The fwg are the modules proposed to be designed in the 'Cyber Shakti': -

(a) **IT Assets Module.** This module will help to manage IT assets issued to all brs. The aim of this module is to manage digital ledger to bring more transparency and accountability to manage and procure IT Assets.

(b) **Fault Control Module.** Currently this HQ has a SW to maintain complaints raised by Brs but the same is not whitelisted and has outdated vintage database. There is a need to have single platform to integrate the assets of IT and raise complaints simultaneously to mitigate the problems of HW or SW in nature.

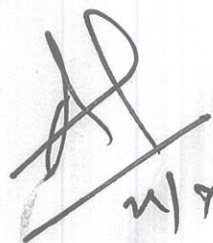
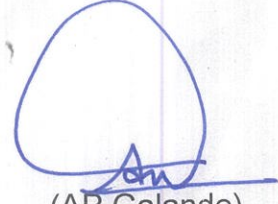
(c) **Cyber Audit.** The aim of this module is that in the existing system auditing team audit the IT Assets held at HQ SC. They run the automated script on client machine and take print out of generated audit report and then finally they assemble all the reports and prepare board which includes observations like critical, high and very high. These reports need to be displayed in graphical manner as per selected fmn. This will ensure the mitigation and record of all Cyber obsn of each asset held with the fmn. The details of the obsn will also be displayed and recorded for future refs.

4. **Estimated Expdr.** Market svy for the same has been carried out at our end from various developers. The estimate has been sought from various SW developers to arrive at approx ~~x~~ expdr for SW devp.

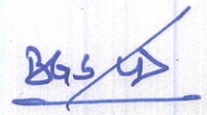

5. **Whitelisting of SW.** Post apvl of CFA, the file will be uploaded on PAW site of DGIS for seeking in principle apvl for the same.

6. PU for perusal & approval of MGGS (SD & CD) pl.

1A
1B
1C

my 43 (SD & CD) ✓ OK. 3  n/r 
(AP Galande)
Col
Col GS (Sys)

25 Sep 2024

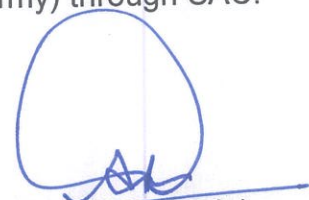
2  Recommended. The module will help to automate the managed of IT assets, fault ngs and cyber audit follow up.  18/10/24

STATEMENT OF CASE FOR WHITELISTING OF SOFTWARE APPLICATION

1. **Unit/Directorate/Office Initiating the Statement of Case.** GS (Sys) Branch, HQ Southern Comd Pune-01.
2. **Aim.** 'Cyber Shakti' appl is proposed to be devp for maint the record of all IT assets and facilitate timely mitigation of any fault or cyber obsn.
3. **Justification.** There are almost 621 computers, 52 MFDs and 46 Internet connections held with HQ Southern Comd. The fmns under HQ Southern Comd also hold no of computer assets due to overall influx of IT into IA. Therefore, there is a need to account for all the IT assets at all fmns carry out timely maint and cyber audit thereby maint cyber hygiene.
4. **Authority.** As per SOP on Whitelisting of Appl Software in IA promulgated vide DDG IT letter No 0331921A/B/04001/Policy/Whitelisting SOP/Vol-II/DDG IT (T &P) dt 28 May 2024.
5. **Broad Purpose.** As per justification mentioned above, software appl developed will be outsourced by HQ Southern Comd, GS (Sys) Branch. This appl will maint the record of all IT assets and facilitate timely mitigation of any fault or cyber obsn raised during Cyber Audit. This SW appl will be a single platform to maint the cyber hygiene of the fmn to avoid duplicacy & transparency. The fwg are the modules proposed to be designed in the 'Cyber Shakti' :-
 - (a) **IT Assets Module.** This module will help to manage IT assets issued to all brs. The aim of this module is to manage digital ledger to bring more transparency and accountability to manage and procure IT Assets.
 - (b) **Fault Control Module.** Currently this HQ has a SW to maintain complaints raised by Brs but the same is of outdated vintage. There is a need to have single platform to integrate the assets of IT and raise complaints simultaneously to mitigate the problems of HW or SW in nature.
 - (c) **Cyber Audit.** The aim of this module is that in the existing system auditing team audit the IT Assets held at HQ SC. They run the automated script on client machine and take print out of generated audit report and then finally they assemble all the reports and prepare board which includes observations like critical, high and very high. These reports need to be displayed in graphical manner as per selected fmn. This will ensure the mitigation and record of all Cyber obsns of each asset held with the fmn. The details of the obsn will also be displayed and recorded for future refs.
6. **Estimated Cost of Proposal.** **Approx 15 Lac.** The software is being developed by outsourcing.
7. **Competent Financial Authority.** DG IS, IHQ of MoD (Army) through SAC.

Case No: 700181/Whitelisting/Cyber Shakti/GS(Sys)

Date : 22 Oct 2024


(AP Galande)
Col
Col GS (Sys)


CHECKLIST

Ser No	Mandatory Details	Particulars
1.	Name of the project	Cyber Shakti
2.	Name of the sponsor	GS (SYS) Br, HQ Southern Comd
3.	Type of Software	Web Appl
4.	Brief justification	There are almost 621 computers, 52 MFDs and 46 Internet connections held with HQ Southern Comd. The fmns under HQ Southern Comd also held no of computer assets due to overall influx of IT into IA. Therefore, there is a need to account for all the IT assets at all fmns as well as carry out timely maint and cyber audit thereby mitigating the obsns to maint cyber hygiene.
5.	Aim, Scope, Purpose incl utility, beneficiary and tgt users	'Cyber Shakti' appl is proposed to be devp for maint the record of all IT assets and facilitate timely mitigation of any fault or cyber obsn.
6.	To be hosted on Internet / ADN	ADN.
7.	Being develop in-house or through IT funds	Outsourcing.
8.	Usability of proposed appl by other arms/services/org/est	Software being developed is generic and can be utilised by other arms/services/org/est
9.	HW and IT Infra reqd	Not applicable. The appl will be hosted on existing server of HQ Southern Comd.
10.	Brief details of content of the proposed SW appl	Frontend: React JS for dynamic user interface. Backend: Java Spring boot for server-side operations and API development. Database: MySQL for robust and scalable data storage.
11.	Endorsement by Head of Branch	Yes. Case file No 700181/Whitelisting/Cyber Shakti/GS(Sys) dt 21 Oct 2024.
12.	Details of user base	All users of HQ Southern Comd.
	(Mandatory for Post Appvl Stg)	
13.	Envisaged cost of entire proj incl license fees and maint.	Approx 15 Lakh
14.	Projected dt of completion incl maj timelines	3 months from the date of Approval
15.	Brief detail iof Sw platform and tech stack proposed for devp of appl incl op sys dependencies (if any).	Frontend: React JS for dynamic user interface. Backend: Java Spring boot for server-side operations and API development. Database: MySQL for robust and scalable data storage.
16.	Brief detail of proposed network and bandwidth reqmt.	Less than 4 Mbps.

Ser No	Mandatory Details	Particulars
17.	Brief details of OS & Sys software reqmts.	Win Server 2022 Std
18.	Brief details of proposed data security measures incl backup of data.	To be integrated with IAM and appln will be hosted on HA platform to maint Backup.
19.	Brief details of proposed database engine to be used in the appl.	MySQL
20.	Details of sw architecture and COTS SW proposed to be utilised.	NIL
21.	Details of proposed architecture – centralised/ federated/hybrid	centralised
22.	Brief details of proposed utilisation of Public Key Infra (PKI) and Iden and Access Mgt (IAM)	SSL & DNS registration will be done on post devp
23.	Technology dependencies (If Any)	NIL
24.	Database reqmts	MySQL
25.	Enhancement/upgradation (Incl Patch mgt / sw updt procedure and mechanism	Vendor to be provide 5 years support
26.	Details of licensing (If any)	NIL

Case No : 0407002F/700181/Whitelisting/
Cyber Shakti/GS(Sys)

Date : 22 Oct 2024


(A P Galande)
Col
Col GS (Sys)
for GOC-in-C

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 cyber shakti 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.



Date : 23 Oct 2024

ब्रिगेडियर (सीडी)
Brig (CD)

मुख्यालय दक्षिण कमान

HQ Southern Command

offg