Tele : 39696

1705005/AFSAC/03566/SDG/ASDC Nov 2024

INTEGRATED HQ OF MoD (ARMY), DTE GEN OF INFO SYS
ARMY SOFTWARE DEVP CENTRE

FUNCTIONAL TESTING OF WEB APPL : ENTERPRISE- INDIAN ARMY SECURE ACCESS CARD APPL (E-ISAC)

1. Pl ref:-

(a) **Functional Testing Clearance** vide ACG SN No B/51106/ArCyGp/T-3/T&E/ E-ISAC dt 14 Nov 2024 even dt 08 Nov 2024 (copy att).

(b) AFSAC Cell letter No A/38024/MI-11/ AFSAC 21 Nov 2024 (copy att).

(c) **Functional Testing Clearance till 30 Dec 2024** vide DGMO/ MO-12 SN No A/12108/Vetting/ MO-12 dt 13 Nov 2024(copy att).

2. Para-wise reply in r/o obsns raised vide ACG SN under ref at para 1(a) are given below:-

Ser No	Ref ACG SN dt 08 Nov 2024	Action
(a)	**Open Ports** under Para 3(a)	Ports blocked
(b)	**Improper RBAC leading to Privilege Escalation** under Para 3(b)	Impl
(c)	**Password Type Input with Autocomplete not Disabled** under Para 3(c)	Disabled
(d)	**Simultaneous Multiple Logins** under Para 3(d)	Restricted
(e)	**Non-Functional Modules/ links** under Para 3(e)	Removed
(f)	**Data Validation** under Para 3(f)	Completed
(g)	**Body Parameters Accepted in Query** under Para 3(g)	Rectified
(h)	**Non-Encryption of Data at Rest** under Para 3(h)	Encrypted
(i)	**System Administrator Acct Config** under Para 3(j)	Renamed
(j)	**Unused/ Commented Code** under Para 3(k)	Removed
(k)	**Misconfig Session Cookie** under Para 3(l)	Rectified
(l)	**Dummy Data (minimum two users each for CO, Adjt, Records)** under Para 4(c)	Test data and users created

3. **AFSAC Cell (letter quoted at para 1(b) above)**. It is intimated that the APIs wrt INDRA & OASIS will be fine tuned during the functional testing and the same will be handed over to ACG (for whitelisting) post completion of functional testing. Also, the Data Cl wrt appl is confd, thus 2FA will be enabled at IAM level.

4. **Appl VDI (along with rectifications mentioned at para 2 above) is fwd for hosting on ADN for necy functional testing by the envt.**

5. For your info and necy action.

Note- The ibid proj is mov only on '**Portal for Appl Whitelisting'** (PAW) for info and n/a of stakeholders except for MO-12, MP-6 & MP-8.

Signed by
Jasjeet Singh
Date: 29-11-2024 14:02:57
(Jasjeet Singh)
Lt Col
GSO-1
for Comdt

Sigs -7 (DG Sigs)

AHCC(DG Sigs)

Copy to :-

HQ DGIS .

AFSAC Cell (DGMI/ MI-11)

MO-12 (DG MO)

ACG

MP-6 & MP-8

RESTRICTED

Tele : 33316/33478

A/12108/Vetting/MO 12 13 Nov 24

DIRECTORATE GENERAL OF MILITARY OPERATIONS (MO 12)

FUNCTIONAL TESTING OF E-ISAC APPL (AFSAC PROJ)

1. **Refs**:-

   (a) DGMO/MO 12 Note No A/12108/Vetting/MO 12 dt 05 Sep 24.

   (b) DGMI/MI 11 (AFSAC Cell) Note No A/38024/MI-11/AFSAC dt 08 Nov 24.

2. Functional testing of E-ISAC application to be completed by **30 Dec 24**.

3. For info and necessary action pl.

(Vishnu Prasad Hota)
Maj
GSO 1 MO 12
for DGMO

DGMI/ MI 11 (AFSAC CELL)

Copy to :-

DG Sigs/ Sigs 7

ACG

AHCC

Internal

MO 10

RESTRICTED

(FUNCTIONAL TESTING CLEARANCE)

Tele: 39707

B/51106/ArCyGp/T-3/T&E/E-ISAC 14 Nov 2024

DTE GEN OF MIL OPS
(ARMY CYBER GP)

FUNCTIONAL TESTING OF WEB APPL: ENTERPRISE- INDIAN ARMY SECURE ACCESS CARD APPL (E-ISAC)

1. Ref the fwg: -

   (a) DGMO (MO-12) office note No A/12108/Vetting/MO12 dt 13 Nov 2024.

   (b) ACG office note No B/51106/ArCyGp/T-3/T&E/E-ISAC dt 12 Nov 2024.

   (c) ACG office note No B/51106/ArCyGp/T-3/T&E/E-ISAC dt 08 Nov 2024.

   (d) ASDC office note No 1705005/AFSAC/03566/SDG/ASDC dt 18 Oct 2024.

2. It is intimated that interim cyber security audit report in respect of E-ISAC web appl has been fwd vide this Gp letter at Para 1(c) above. **The same may pl be treated as functional test clearance.**

3. Apropos, the fwg actions are requested to be carried out: -

   (a) **Mitigation of all instances of vulnerabilities highlighted vide letter at Para 1(c) above.**

   (b) **A self-signed certificate** be fwd by the sponsor confirming mitigation of all highlighted obsns under intimation to DGMO (MO-12) and this Gp.

   (c) **Security cl** of data handled by appl and version be intimated to this Gp.

4. Functional testing of appl has been concluded and post expiry of the validity of Functional Test as granted by DGMO/MO-12 (i.e. 30 Dec 2024), **appl to be fwd to ACG for undertaking comprehensive cyber security vetting as per existing SOP on Whitelisting of Appl Sw in IA.**

5. For your info and necessary action pl.

Sd/x-x-x-x-x--x
(NK Verma)
Lt Col
Offg Staff Offr
for Cdr

ASDC

Copy to: -

DGMO (MO-12)
AFSAC Cell (DGMI/MI-11)
DGIS
DDGIT
- For info pl.

RESTRICTED

Tele : 34370

AFSAC Cell,
DGMI/MI-11
IHQ of MoD (Army)
New Delhi-110011

A/38024/MI-11/ AFSAC

21 Nov 24

DGMO/ ACG
DGIS/ ASDC
DGMP/ MP-6&8

POST PSTN COMMENTS WRT FUNCTIONAL TESTING OF E-ISAC APPL (AFSAC PROJ)

1. PI ref the fwg :-

   (a) This office letter No A/38024/MI-11/AFSAC dt 18 Jul & 08 Nov 24.

   (b) DGMO/ MO-12 ION No A/12108/Vetting/MO 12 dt 05 Sep & 13 Nov 24.

   (c) DGMO/ ACG ION No B/51106/ ArCyGp/ T-3/ T&E/ E-ISAC dt 12 & 14 Nov 24.

2. A **pstn on E-ISAC was conducted on 07 Nov 24 by ADSC to ACG** for cyber vetting of the appl. It is highlighted that in the ibid pstn the **Sponsor Dte (DGMI/ AFSAC Cell) was neither info nor was part of the dscn**. IA AFSAC proj is a complex High Risk High Security proj involving various stakeholders wherein DGIS is one of the stakeholders of the proj for devp of E-ISAC appl. The **developer i.e. DGIS/ ASDC** apparently was not aware of the overall scheme of proj involving other stakeholders due to security reasons.

3. Para-wise reply to aspects pertaining to E-ISAC Web appl as mentioned at Para 3 & 4 of your letter under ref above are given below:-

S No	Aspects	Comments by AFSAC Cell/ MI-11	Action By
(a)	Data Encryption/ Tokenisation	Data at rest will be stored on AHCC servers and SHA 256 or above protocols will be complied with.	ASDC/ DGIS to confirm to ACG that action is complete.
(b)	Impl of 2FA	The appl will be handling PII data along with Token identifiers which makes it confidential. The entire ORBAT is not visible to any user. Only the Admins are allowed to have visibility of the full Data who will use 2FA to login and a digital log is also maint by the appl of the same.	ASDC/ DGIS to confirm to ACG that action is complete.
(c)	Integration with other appls	Whitelisted API Gateway (devp by MISO) is being used for integration with other appl.	ASDC/ DGIS to confirm to ACG that action is complete.

S No	Aspects	Comments by AFSAC Cell/ MI-11	Action By
(d)	Role Based Access	User roles will be shared with ACG by the developer ASDC.	ASDC/ DGIS to confirm to ACG that action is complete.
(e)	Latest Version	Latest version of devp platform and third-party comps will be dply/utilised/upgraded to.	ASDC/ DGIS to confirm to ACG that action is complete.
(f)	Storage of AADHAAR No	The decision has been taken at VCC and CISC mtgs in 2022. Requisite permission has been taken from UIDAI HQ as per the AADHAAR Act. **Complied with.**	AFSAC Cell/ DGMI. **Action is completed**.
(g)	Export of data from E-ISAC Appl	The procedures and resp of exporting of data was finalised in AG's Conf on 22 Feb 24 where in it was decided that data will be shared in encrypted format in secure drive moreover to ensure physical security the printing will be done in front of AFSAC Offrs and data will be destroyed post printing of AFSAC and a certificate will be rendered by the agency countersigned by the state Police/ IB. **Complied with.**	AFSAC Cell/ DGMI. **Action is completed**
(h)	Logging Mechanism	To be complied with.	ASDC/ DGIS to confirm to ACG that action is complete.
(j)	Data Retention	No data will be stored beyond a permissible limit by the sponsor or any stakeholder. Same was agreed to in AG's Conf. Pt **complied with**.	AFSAC Cell/ DGMI ASDC/ DGIS. **Action is completed**
(k)	Digital Watermarking	**Complied with**.	ASDC/ DGIS to confirm to ACG that action is complete.
(l)	Vetting of Associated Appl	To be complied with.	MP-6&8 to confirm to ACG that action is complete.
(m)	Security of Exported Data	Ref sub para (g) above. **Complied with.**	AFSAC Cell/ DGMI. **Action is completed**
(n)	Data Security at Printing Agency	Ref sub para (g) above. **Complied with.**	AFSAC Cell/ DGMI. **Action is completed**

4. **Only for ASDC/ MP-6&8**. ACG has requested a certificate to be fwd confirming mitigation of all highlighted obsn vide DGMO/ ACG letter No B/51106/ ArCyGp/ T-3/ T&E/ E-ISAC dt 12 Nov 24. A **certificate is att as Appx** to be signed by ASDC and MP 6&8 for the same.

5. It is requested that any pstn/ mtgs related to AFSAC incl e-ISAC if conducted in future; the sponsor dte to be info and to be incl in dscn. You are requested to pass **necy dirn for hosting of E-ISAC for functional testing on ADN** post resolution of the queries (If any) latest by 22 Nov 24.

6. An early action is requested pl.

Sd \-X-X-X-X
(AS Rana)
Lt Col
Proj Offr, AFSAC Proj
for DG MI

Appx :- Format of Cert of Compliance

Copy to:-

DGIS/ MISO
Sigs-7 & AHCC
- for info pl.

RESTRICTED
INTERIM REPORT

Tele: 39707
B/51106/ArCyGp/T-3/T&E/ E-ISAC 08 Nov 2024

DTE GEN OF MIL OPS
(ARMY CYBER GP)

CYBER SECURITY AUDIT OF WEB APPL: ENTERPRISE- INDIAN ARMY SECURE ACCESS CARD APPL (E-ISAC)

1. Ref the fwg: -

   (a) ACG note No B/51106/ArCyGp/T-3/T&E/ E-ISAC dt 05 Nov 2024.

   (b) ACG note No B/51106/ArCyGp/T-3/T&E/ E-ISAC dt 28 Oct 2024.

   (c) ASDC note No 1705005/AFSAC/03566/SDG/ASDC dt 18 Oct 2024.

   (d) ACG letter No B/51106/ArCyGp/T-3/T&E/Adv1 dt 24 Aug 2023.

2. The VDI of the web appl **"E-ISAC"** handed over to ACG after initial config by developer rep on 01 Nov 2024 was analysed for cyber security compliance as per the dirns laid down in the Army Cyber Security Policy (ACSP)-2023.

3. Detls of vulnerabilities obs during current iteration are as under: -

   (a) **Open Ports**. A No of open ports were detected on the web server. The screenshot for the same is att as **Appx A**. **Suggested mitigation methodology is to block all other ports except the port used by web server by implementing firewall rules**.

   (b) **Improper RBAC leading to Privilege Escalation**. It has been obs that RBAC has not been properly impl in the appl. In the present state, a non-admin user can update profile of an admin user. Screenshot is att at **Appx B**. **It is strongly 'R' to impl RBAC on all modules incl in the appl as per envisaged role of regd users**.

   (c) **Password Type Input with Autocomplete not Disabled**. The user end web browser has the built-in functionality of remembering user input in the form of username and password. Screenshot of the same is att as **Appx C**. This functionality results in storage/ caching of vital user credentials on the client machine (browser cache) and the same can be subsequently exploited. In the ibid application, autocomplete functionality for Password has not been set to off. Suggested mitigation methodology is to disable this functionality wherein the option of password auto complete is not avbl to the user.

   (d) **Simultaneous Multiple Logins**. In its present state, the appl has not been configured to ensure unique login of users. This is exhibited by the ability of a user/ admin to login into the sys from multiple devices simultaneously. Screenshot of the same is at **Appx D**. To ensure the requisite std of cyber security, **it is strongly recom that the login of user credentials be restd to a single instance only. The latest session established with a particular user ID should be maintained and all previous sessions should be terminated**.

(e) **Non-Functional Modules/ links**. It is obs within the web appl that some of the modules/ links are non-functional. "Fetch Data from DB" while applying for new I-card is not functional in the appl. The screenshot is att at **Appx E**. Suggested mitigation methodology is to carry out appl wide mitigation of similar vulnerabilities and all modules/ functionalities linked with the appl as per its final dply.

(f) **Data Validation**. It is obs that server error msg is being generated by the web appl on supplying malformed inputs which indicates presence of faulty appl code. Screenshot is att at **Appx F**. Necessary controls wrt user input validation have not been impl within the subject web appl. **It is 'R' to validate the input fds against type, length, format and rg of data and iden and correct all such instances of code**.

(g) **Body Parameters Accepted in Query**. It is obs that body parameters are accepted in the URL within the devp web appl. List of URLs is att as **Appx G**. Attacking query parameters sent via GET requests is easier than body parameters sent via POST requests. Suggested mitigation methodology is to use POST requests to submit data to the appl and to ensure that body parameters sent via query string are not accepted by the appl.

(h) **Non-Encryption of Data at Rest**. In present status Army No, Mobile Nos etc are being stored in clear format in the database. The screenshot of the same is att as **Appx H**. **Suggested mitigation methodology is to ensure that all sensitive data is identified and secured at rest with latest secure encryption methods**.

(j) **System Administrator Acct Config**. Default System Admin acct 'sa' has been obs in the database. Screenshot is at as **Appx J**. The sysadmin acct is vulnerable in its default configuration as it can be exploited to perform unauth activities on the web appl database. **It is 'R' to rename the SA acct and to change the password for SA and other logins on a regular basis**.

(k) **Unused/ Commented Code**. It is obs that instances of unused code are present within the source code of the web appl. Screenshot is att at **Appx K**. **It is 'R' to remove the unused/ commented code and appl wide mitigation be undertaken**.

(l) **Misconfig Session Cookie**. It is observed that a dummy cookie named "MySecureCookie" with a default static value of "cookieValue" is being assigned to all users. Screenshot is att at **Appx L**. **It is 'R' to reconsider usage of ibid session cookie**.

4. Apropos, the fwg actions are requested to be undertaken by the sponsor/ developer: -

(a) Mitigation of all instances of aforementioned vulnerabilities in the appl.

(b) Post mitigation fwd vulnerability wise mitigation methodology alongwith screenshots for the better understanding of the Test Team.

(c) **Dummy Data**. The VDI submitted for lab test to be populated with dummy data for all roles (minimum two users each for CO, Adjt, Records).

5. Ref letter mentioned at Para 1(d), sponsor should info the IP addr of the machine from where the remote mitigation of highlighted vulnerabilities will be undertaken so that the same can be whitelisted in the ACG firewall. **In the absence of intimation of any prog for three months from the date of issue of this letter, the website/appl Security Vetting case will be deemed to be closed**.

6. A Compendium of advisories is hosted at Army Cyber Gp on the link "*Web Development > Test & Eval Advisories*", as a ready reckoner, which will assist the developer in addressing the security issues in the website/ web appl. It is requested that same be ref to seek necessary assist. Also, a **mitigation asst desk** has been est at Army Cyber Gp where the developer rep can clarify any issues in the VA report and undertake in-situ mitigation of vulnerabilities.

7. For info and necessary action pl.

Sd/x-x-x-x-x-
(Manmeet Singh)
Lt Col
Staff Offr
for Cdr

Encls. As above

ASDC

Copy to: -

DGMO (MO-12)
AFSAC Cell (DGMI/MI-11) } - For info pl.