REQUEST FOR INFORMATION (RFI)

For

“COMPOSITE SMART CARD”
FOR ARMED FORCES PERSONNEL AND THEIR DEPENDENTS

RFI can be downloaded from the website : HQ IDS Website

Last date and time of receipt of input : 4:00 PM on 26 Aug 2015

Address for submission & Vendor Interaction : HQ IDS (Med)
Wing 7, West Block-III,
Ground Floor, R.K. Puram,
New Delhi-110066

Medical branch, HQ Integrated Defence Staff

New Delhi
REQUEST FOR INFORMATION (RFI) FOR “COMPOSITE SMART CARD”
FOR ARMED FORCES PERSONNEL AND THEIR DEPENDENTS

1. The Deputy Chief IDS (Med), Ministry of Defence, Government of India, intend to introduce multi-application 'Composite Smart Card for Serving / Retd Armed Forces Personnel and their dependents (approx 110 Lakhs) for improving the medical and CSD facilities. The card will also act as Identity card for Ex-servicemen and dependents of serving personnel / Ex-Servicemen.

2. The “Composite Smart card” project will also require development of software, and purchase of hardware and peripherals for its use. This will be BOOT model project. Approximate quantity of hardware and peripherals required is given in the Para 14 of the RFI document.

3. The details of complete requirements from vendors are given in the RFI document. Interested parties / vendors are requested to forward information on the work they can undertake. The broad specifications and requirements are given in the Annexure “I”. In addition the responders are also requested to furnish details as per the pro-forma at Annexure “II”.

4. The requested information may please be forwarded to the under mentioned address by 26 Aug 2015 at 1600 hrs.

O/o Deputy Chief IDS (Med),
Wing -7, Ground Floor, West Block-III,
R.K. Puram, New Delhi - 110066
Tele: 011-26169079/ 011-26169317
Fax: 011-26712407
Email ID: dirit.idsmmed@nic.in, Jtdirit.idsmmed@nic.in

Sd/xxxxxxxx
(Mahender Kumar)
Col
Dir IDS (Med Info)
For DCIDS (Med)
REQUEST FOR INFORMATION (RFI) FOR “COMPOSITE SMART CARD”
FOR ARMED FORCES PERSONNEL AND THEIR DEPENDENTS

1. The Deputy Chief IDS (Med), Ministry of Defence, Government of India, intend to introduce multi-application ‘Composite Smart Card for Serving / Retd Armed Forces Personnel and their dependents (approx 110 lakhs) for improving the medical and CSD facilities. The card will also act as Identity card for Ex-Servicemen and dependents of serving personnel / Ex-Servicemen.

2. Information is solicited from OEMs / vendors / system integrators of smart cards solutions with regards to various aspects of Smart Cards including but not limited to the memory capacity, security, tamper resistance, feasibility of integrating with existing legacy applications technical/ administrative challenges therein and hardware’s required to use Composite Smart Cards, etc. so as to provide a Single integrated solution for identity management, authentication, medical and canteen data storage management using PIN and bio-metrics (fingerprint) based Smart Cards.

3. This Request for Information (RFI) consists of two parts as indicated below:-

(a) **Part I.** The first part of the RFI gives an overview of the existing system, the proposed operational characteristics and features, technical and administrative requirements in the new smart card based system and the draft scope of work.
(b) **Part II.** The second part of the RFI states the methodology of seeking response of vendors. Submission of incomplete response format will render the vendor liable for rejection.

PART- I

4. **Intended Use of Composite Smart Card/ Equipment (Operational requirements).** The "Composite Smart Cards" including Health Smart Card, CSD smart card and ECHS smart card incorporating automation of complete workflow of the Service Hospitals, CSD and ECHS polyclinics is required. This card will also be used as ID card for Ex-serviceman and dependents of serving and Ex-servicemen. (The cards will also implement changes in policy decisions of respective services from time to time).
5. **Important Technical parameters.** The broad tentative technical requirements placed at Annexure I.

6. Vendor should confirm that following conditions are acceptable:-

   (a) The solicitation of offers will be as per 'Single Stage-Two Bid System". It would imply that a 'Request for Proposal" would be issued soliciting the technical and commercial offers together, but in two separate sealed envelopes. The validity of commercial offers would be at least 18 months from the date of submitting of offers.

   (b) The technical offers would be evaluated by a Technical Evaluation committee (TEC) to check their compliance with RFP.

   (c) The Proposal of all TEC cleared vendors would be put through a trial evaluation in India on a "No Cost No Commitment" basis. A staff evaluation would be carried out by HQ IDS (Med), CS Directorate and MD central Org ECHS to analyze the results and shortlist the vendors.

   (d) After clearance by the Evaluation Team, a Contract Negotiation committee would decide the lowest cost bidder (L1) amongst the technically compliant offers and conclude the appropriate contract.

   (e) Vendor would be bound to provide product support in terms of a comprehensive Maintenance Contract as per the time period and terms & conditions specified in RFP.

   (f) The vendor would be required to accept the general conditions of contract given in the Standard Contract Document at Chapter V of DPP 2013 placed on [www.mod.nic.in.](http://www.mod.nic.in)

   (g) **Offset Clause.** The vendor will need to undertake offset contracts amounting to 30 % of the value of commercial proposals, if applicable.

   (h) **Integrity Pact.** An integrity pact along with appropriate EMO would need to be submitted, if applicable (refer Annex / to Appx H of schedule-I of Chapter-I of DPP 2013).

   (i) **Performance-cum-Warranty Bond.** Performance-cum-Warranty Bonds are required to be submitted after signing of contract as per provisions of OPP 2013.

   (j) **ToT.** The technology including the entire source code is to be handed to HQ IDS, MoD is desirous of Source Code for the core application software content of the system.
PART-II

7. Procedure for Response

(a) Vendors must fill the form of response as given in Appendix E of Chapter I of DPP 2013 (copy placed at Annexure II & Annexure III). Apart from filling information about the company, details about the exact product meeting the generic technical specifications (defined in Annexure) should also be carefully furnished. Additional literature on the system can also be attached with the reply. The RFI is to seek information on products that are available with the vendor. Deviations in parameters are acceptable at this stage and flexibility is possible. Other additional features if available may be indicated as optional equipment.

(b) The filled form should be dispatched to under mentioned address:

O/o Deputy Chief IDS (Med),
Ministry of Defence
Wing -7, Ground Floor, West Block-III,
R.K. Puram, New Delhi - 110066
Tele: 011-26169079/ 011-26169317
Fax: 011-26712407
Email ID: dirit.idsmmed@nic.in, Jtdirit.idsmmed@nic.in

(c) Last date of acceptance of response is 26 Aug 2015 by 1600 hrs. However, amplification if any can be provided subsequently.

8. The Government of India invites responses to this request only from Original Equipment Manufacturers (OEM)/ Authorized Vendors/Government Sponsored Export Agencies (applicable in the case of countries where domestic laws do not permit direct export by OEMs). A confirmation to this effect is requested in the response. The end users of the Composite Smart Card/ equipments are the Hospitals, CSD Canteens and ECHS Polyclinics.

9. Vendor is to clearly state in his proposal, if the system is already in use or under development and state the plan and timelines for providing the system. Necessary government clearances would need to be obtained, where applicable, by the vendor for supply of the equipment to Govt of India.

10. The vendor is to attach detailed technical specifications of the Composite Smart Card/ equipment being offered. For planning and budgeting, the vendor is requested to provide a rough order of magnitude cost of the system under following options:

(a) Total Cost of Smart card and software without hardware, indicating cost of each card.
(b) Total Cost of direct purchase of the composite cards, computers, servers, peripherals, other hardware, installation of system and integration with pre-existing HIS, ECHS and CIMS systems all together and cost of individual card in this model.

(c) Cost of warranty for 5 years and annual comprehensive (including all spares) maintenance support along with terms and conditions for the performance based support for next 5 years (total 10 years of onsite comprehensive warranty and AMC)

11. This information is being issued with no financial commitment and the Ministry of Defence reserves the right to change or vary any part thereof at any stage. The Govt of India also reserves the right to withdraw it should it be so necessary at any stage. The Acquisition process would be carried out under the provisions of DPP 2013.
Annexure-I
(Refers to Para 4 of RFI)

TENTATIVE TECHNICAL REQUIREMENTS FOR PROJECT
“COMPOSITE SMART CARDS (CSC)”

Purpose

1. The "Composite Smart Cards" including Health Smart Card, CSD smart card and ECHS smart card incorporating automation of complete workflow of the Service Hospitals, CSD and ECHS polyclinics is required. This card will also be used as ID card for Ex-serviceman and dependents of serving and Ex-servicemen. (The cards will also implement changes in policy decisions of respective services from time to time).

2. Design, develop and issue of Composite Smart Cards to serving personnel, ECHS, and CSD beneficiaries and their dependents which must meet following functional criteria's:-
   (a) Populate all the data fields in HIMS during registration of patients at hospitals.
   (b) Authenticate the identity of card holder using bio-metrics.
   (c) Store Medical and CSD transaction data which can be viewed at other locations.
   (d) Secure medical and CSD transactions which should be allowed only in presence of beneficiary and operator’s card.

3. The Composite Smart Cards should be able to work on client based standalone computer, LAN as well as on the WAN/ respective Service Intranet. The cards will identify users by biometric finger printing method at hospitals and ECHS polyclinics and via Biometric or Security key (PIN) at URC counters the user photograph will be common to all. The cards will store medical data and CSD data on the chip. The data will be editable at respective locations of Hospitals, URC and ECHS polyclinics, using specific software only.

4. This project will follow the BOOT model i.e. Build, Operate, Own and Transfer model of public private partnership in Govt projects. The vendor will start the project at his own cost, provide necessary HW and SW and install them at requisite places and start delivering the cards. The HW and SW will be operated by the vendor and meet the minimum requirements of uptime at all times over a period of ten (10 yrs) years.

Architecture

5. The Smart card and software should be capable of being hosted on the existing network maintained by Defence. The hardware and software for the project should seamlessly integrate into the existing network architecture. No separate networking infrastructure should be required for the project.
6. The Smart card and software should be on secure web based architecture. The database of individual user should be there on his own Composite Smart Card. The application and the complete databases would be residing on individual PCs not connected via LAN/ Internet, servers located locally as well as remotely when connected via service intranets and internet. The operating platform in use should be Windows 8.1 or higher (latest available in the market). The Users would access the application through secure web browser with comprehensive access rights management module for ensuring data integrity and data security.

7. The Smart card and software should have in-built security features and key management systems so that only authorized person can access or edit the data i.e. rep at hospitals should not be able to access data of ECHS and CSD, ECHS rep should not be able to see Hospitals records and CSD data, and similarly CSD rep should not be able to see Hospital and ECHS data/ records. It implies that rep at one service end should be able to view and edit data/ record of his department only and the data of other departments should be inaccessible to him.

Features

8. Composite Smart Card must be a contact smart card and have smart features with minimum 128 Kb memory, SCOSTA certified by NIC and Should have 256 bit AES encryption i.e. ISO/IEC18033-3 standards compliant. The SCOSTA certification of 128 Kb card from NIC will be responsibility of the vendor. It must help in identifying the CSC holder by displaying soft copy of his/her photograph stored on the CSC and authenticating the identity by matching fingerprints stored on the CSC with that of fingerprints read by biometric reader installed at reception of hospitals. The process of authentication by matching the fingerprints should not take more than three (03) seconds. The chip should have lifetime data retaining capacity. The chip should have sufficient space to retain CSD data & HIS data of minimum 10 years and remaining free space for future expansion.

9. The card will cater for two major functionalities i.e. HIMS (for ECHS and Hospital module) and CIMS (for canteen management). The application should be modular to allow processing of technical & administrative information and integration of other modules and system databases. The application should be able to integrate with existing legacy automation systems of CSD (i.e. CIMS-Canteen Inventory management software) and ECHS polyclinics.

10. The basic overview of the proposed system is shown below:-
11. The Multi-Application integration and authentication in Composite Card Software should be:

![Composite Card Diagram]

12. Security mechanisms for partitioning of data should be implemented within smart card OS as well as in respective applications such that a smart card reader authorized for one application can read only its relevant data and not other modules data (common data will be readable from all authorized terminals).

13. The authorization to access the card should be BIOMETRIC authentication for ECHS & Hospital module but biometric and 4 Digit PIN for CSD module, as depicted in para 9 above.

14. List of items / services required is as follows:-

<table>
<thead>
<tr>
<th>S. No</th>
<th>Name</th>
<th>Type of item/services/description</th>
<th>Qty required</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>Customized Composite Smart Cards</td>
<td>Micro-processor based Integrated Circuit cards. Preferred chip – NXP/Infineon/Samsung/ST Micro/Smart chip/ Manipal Technologies Pvt Ltd/Coresonant System/ Shreenath Smart Technology etc. CPU – Secure CPU Architecture Memory size for user (EEPROM) –128 KB or more. Memory size for code (ROM) - 80 KB or more. RAM – 4K or more. Should be compliant to SCOSTA v1.2b dated 15 Mar 2002, including all addendums and errata and compliant to ISO/IEC 7816 for contact smart cards. Minimum 10 years of life for data retention. Operating ambient temperature range: - 25(^\circ) to 55(^\circ) C.</td>
<td>+ 1,10,00,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Supply voltage: 1.6 to 5.5V  
Interface – ISO/IEC 7816 T=0 or T=1 transport protocol.  
Should have AES encryption. ISO/IEC18033-3 standards compliant.  
Endurance – 5,00,000 programming cycles  
Certification – EAL 5+, FIPS 140-2 level 3, PP0035 certificate  
OS – SCOSTA with lifetime licensing  
OS Burning – Hard masking at chip manufacturing stage  
Should have PVC plastic constructed 4 layers.  
Laminated card body with two layers of PVC printing and 2 layers of PVC overlay to allow color dye sublimation printing.  
Operating system manual and chip technical manual should be provided.  
256 bit AES, ISO/IEC18033-3 Security standards. |
| **(b)** Smart Card Readers with interface Software | Factory standard for PC to Smart Card Reader interface.  
ISO 7816 compliant.  
Should support 3V chip card with T=0 and T=1 transport protocol.  
Should have external USB interface.  
Must have Factory standard for PC to Smart Card Reader interface drivers. |
Pixel resolution: minimum 197dpcm/ 512 dpi.  
Scan capture area: >=14.6mm x 18.1 mm  
Scan data: 8-bit gray scale.  
Should have USB interface (USB 2.0).  
Supply voltage: 5.0 V ±5%.  
Comply with BioAPI specifications Or ISO/IEC 19784-1/4 compliant.  
The duplicate check during the enrolment and implementation phase will use 1: N matching.  
| **(d)** Software CSC | CSC software to be operated on standalone PCs / Local Server, LAN, Intranet and Internet using  
20385 |
|   |   | 21904 |
| (e) | PCs | CPU – Intel Core i3-3220, 3.3 GHz, 3 MB Cache or higher  
     |     | Chipset – Intel 6 series or better  
     |     | Bus Architecture – 3 PCI or more  
     |     | Memory – 4 GB 1333 MHz DDR3 RAM  
     |     | Hard Disk Drive – 500 GB 7200 rpm or higher  
     |     | 47 cm or larger TFT/LED digital color monitor TCO certified  
     |     | Keyboard – 104 keys  
     |     | Mouse – optical with USB interface  
     |     | Ports – 6 USB ports (min 2 in front), 1 serial audio ports for microphone and headphone in front  
     |     | Cabinet – Mini tower  
     |     | DVD ROM Drive – 8X or better  
     |     | Networking facility – 10/100/1000 on board integrated NW port  
     |     | Operating System – Windows 8 professional or above preloaded with media and documentation  
     |     | OS certification – Windows 8.1 OS or above  
     |     | Power Management – Screen blanking, Hard Disk & System idle mode in power on, Power supply SMPS Surge protected |
| (f) | Servers | CPU: Intel xenon 3.3 GHz Quad Core Processor with 15 MB Cache memory  
      |     | Motherboard: Intel series compatible with Intel Xenon 3.3 GHz Quad Core processor  
      |     | Expansion slots: PCI Express 2.0x 16(Min PCI slot2)  
      |     | Enterprise memory: 8 GB DDR3 RAM and min 4 slot (min 16 GB) Enterprise memory, upto 1 TB of 1066 MHz DDR3 Active memory expansion  
      |     | Hard Disk Drive: 1 TB or more.  
      |     | Integrated ports: 3 USB, 2 HMC, 2 SPCN  
      |     | Integrated PCI adaptor slots: 6 PCIe Gen 2 slots  
      |     | Integrated SAS controllers: 02 SAS DASD/SSD controllers, 01 SATA media controller  
      |     | High bandwidth PCI Adaptors: 6Gigabit SAS, 8 Gigabit Fiber channel over Ethernet 40 Gigabit QDR sockets, 4 integrated Media Bays, 01 slim line for SATA DVD RAM  
      |     | Cabinet: Rack mounted  
      |     | Certifications: Red Hat Networking Dual LAN |
Network Card with asset feature
Power requirement: Operating voltage 200V AC, power consumption 1925 watts per enclosure
RACK with cable manager and power DB & Fan

(g) Card and PIN pad readers
Factory standard for PC to Dimension: 5”x3”x2” (10% variation in size would be acceptable)
Wt. : <250 Gms
Operating temp: -250 to 550
Should support 1.6 to 5.5V chip cards with T=0 and T=1 transport protocol.
Should be ISO 7816 compliant
Should support T=0, T=1 transport protocol
Should have external USB interface.
Must have Factory standard for PC to Smart Card Reader interface drivers.

(h) UPS
1 KVA UPS
600VA UPS

(j) Printer
Dot Matrix printer / Laser Jet Printer
Bill Printer

Note: - The vendor may suggest configuration of Hardware, accessories and peripherals as per his own card requirement / solution being provided, but the hardware technology should be latest in market.

15. The Smart card and software application should include but not limited to the following basic modules to function as Health smart card, ECHS card and CSD smart card:-

15.1 HOSPITAL/ HEALTH SPECIFIC DATA:

(a) Armed Forces Medical Services have various hospitals all over the country which can be categorized as under:-

(i) RAP/MI Rooms. RAP/MI Rooms (Medical Inspection Rooms) with one Medical Officer authorized at Battalion level or certain places where size of garrison is small. Here, only general OPD consultations and dispensing of the medicines is done.

(ii) Peripheral/Field Hospitals. Peripheral/Field hospitals are very small hospitals which are authorized more than one Medical officer with basic investigation facilities like X-Ray and Laboratory.
(iii) **Small hospitals with basic specialty.** These are hospitals with specialist care facilities like medicine, surgery, obstetrics and gynaecology, pediatrics etc.

(iv) **Zonal Hospital:** These are bigger hospitals with almost all specialties but no super specialties.

(v) **Super specialty Hospital:** These are super specialty hospitals mainly in large metros.

(b) Three services of Armed Forces and different military hospitals have developed their own HIMS (Hospital Information Management system) application using different vendors, different platforms and database systems. Secondly, Army and Navy do not have enterprise wide HMIS. Air Force has enterprise wide HMIS for its smaller hospitals (Station Medicare Centers), MI Rooms and Dental Centers called the IAF MEDNET and HIS for all its hospitals, both these applications are AFNET based.

(c) The smart card should retain health data of the card holder for minimum latest 10 visits. For the serving personnel the card should have records for Last OPD visits, lab reports, last PME/AME (including lab, radiology Investigation reports and ECG reports as applicable ), Medical category, opinion of specialist if in Low Med cat, Medical Due date alert, Current medical situation, latest Discharge summary, Family medical history, personal history, allergy history, history of any Cardiac problem, history of Hypertension, Diabetes mellitus etc. and other relevant medical history and other data fields which will be specified in RFP and demanded at the time of preparation of SRS/ implementation of software or during customization of software.

(d) The medical data on card should be accessed and edited only at the hospital site, the data should propagate in AFMS Hospital Information Systems (different HIS of Army Hospitals, Navy, and AFNET and other Air Force HIS) automatically and data should be updated automatically in the HIS as well as in the card on contact with card reader.

(e) The card should be accessed by Biometric fingerprint authentication, and hospital rep should be able to view and edit hospital data only.

(f) In case the fingerprint of patient cannot be taken, in that situation the Officer In-charge should have right to register that patient without fingerprint, and that log should be available in the hospital records as well as on the card.

(g) In case the patient forgets to bring his Composite smart card the system should be able to register him for treatment by authenticating his identity from the local server. No patient should be denied treatment.
(h) Data exchange between Composite Smart Card and HMIS/HIS/DIS/ IQMP should be such that the latest data get populated from one to another. Read+ write of medical data should not take more than 5 seconds.

(j) CSC must automatically become invalid for use once the CSC holder ceases to be authorized client of AFMS e.g. a Short Service Commission Officer leaving the service, on PMR (Premature retirement)/ superannuation/on being invalidated or boarded out of service, a son attaining 25 yrs of age etc. In case, a card is reported to be lost/damaged, it should be deactivated and database at all places should be updated so that an un-authorized person doesn’t misuse it. Similarly, database at all places should be updated about other events mentioned above.

15.2 ECHS SPECIFIC DATA

(a) **General**

(i) Ex-Servicemen Contributory Health Scheme (ECHS) was approved by the Government in the year 2003. All defence pensioners who have retired prior to 31 Mar 2003 can voluntarily join the scheme. However all persons retiring on or after 01 Apr 2003 have to join the scheme compulsorily. There are approximately 47 lakh beneficiaries of the scheme who hold a Smart Card issued by ECHS during the last decade. These cards are of two versions 16KB/32KB. There are 426 ECHS Polyclinics in India and 06 in Nepal which are providing the health care services. These are in turn grouped under 28 Regional Centers distributed geographically to exercise control over these polyclinics. Each Polyclinic is affiliated to a Service Hospital and/or group of Diagnostic Centers and/or Empanelled Hospitals, to whom the ECHS members would be referred by the Polyclinic. Every year approx Four Lakhs beneficiaries join the scheme.

(ii). The facility is available for only registered retired defence pensioners / widows and their dependants (under given conditions) who join the scheme by paying a one-time charge as laid down.

(b) **ECHS Smart Card Application.** The Department requires an application that interacts with Smart Card and the ERP being deployed for management of the ECHS organization, the Bill Processing Agency’s Portal and authentication requirements at the Health Care organizations (HCO). The Tenderer is required to study the system and put-up the SRS for the Application within 30 days of awarding of the contract.

(c) **ECHS SYSTEM OBJECTIVES.** The new Smart Card system is aimed at :-
(i) Smart Card (Contact less proximity identification and Biometric Authentication) based system to ensure smooth running and security of the ECHS System and that no unauthorized person avails of medical benefits.

(ii) The ECHS Members are to be identified using contact less proximity card authenticated by biometric, Aadhar based system to prevent fraud at Polyclinics and all the HCOs.

(iii) Build-up of a reliable ECHS Smart Card Application System for ECHS.

(d) PROPOSED SYSTEM (Collection of Data, Personalization & Issue of Smart Card)

(i) The joining members will fill up required form and deposit their contributory member fee through MROs./collected at respective records/PCsDA

(ii) The Station Headquarters will collate and authenticate the data filled in by the member and forward the same to Regional Centers.

(iii) The Tenderer will collect the filled data forms from the Regional Centers and deliver the personalized Smart Card along with a CD containing all the details of the form, photographs to Regional Centers within 30 days of collection. Validation shall be done as per parameters given before personalizing and printing the card.

(iv) The Regional Centers will forward the smart cards to the respective Station Headquarters.

(v) The whole process from collection of form from Regional Center till supply of Smart Card shall take place within 30 days.

(vi) The Tenderer will establish the required infrastructure for the production of ECHS Smart Card. The infrastructure to include civil, electrical, environment and IT, any other facility required to manage the production and distribution of the smart card.

(vii) The Tenderer will ensure all data pertaining to ECHS Smart Card is replicated to Data Centre of ECHS established at Central Org ECHS in real time. For this a dedicated Leased Line of at least 8 Mb/s will be established by the Tenderer between his production facility and Data Centre of ECHS. All
expenses relating to establishment of Leased Line and maintenance shall be borne by the Tenderer. The annual rental in case of hired circuit shall also be borne by the Tenderer.

(e) **Activities at Polyclinic**

(i) The Tenderer will establish the authentication Kiosks @ 1 per 50 footfalls on each polyclinic subject to a minimum of two readers and maximum of 20.

(ii) The beneficiaries would be identified on arrival by the contact less proximity smart card system and authenticated by the Biometric Reader; Aadhar based authentication system by seeding of aadhar data would also be incorporated in the system. On authentication a welcome note will be displayed along with the photograph of the beneficiary at the Kiosk. Beneficiary would be given four options to select on the touch screen panel. Once the selection is made a token would be printed at the kiosk, which will indicate the name of the doctor/counter and time of appointment for the beneficiary.

(iii) If the beneficiary has come to the polyclinic for the first time, his fingerprint will be captured and written into his Smart Card. Smart Card will be activated only after Finger prints information is captured into the Smart Cards.

(iv) On all subsequent visits the contact less proximity smart card system identifies the beneficiary and fingerprint reader /Aadhar No. authenticates. The time taken for this identification and authentication process should not exceed five (5) seconds and the level of accuracy required is 99 percent.

(v) Once authenticated, all personal information read from the Smart Card along with his/her photograph fetched from the Polyclinic database/Central Data Centre and will be displayed on the kiosks.

(vi) In certain cases assistances may be required to be rendered to some beneficiaries. Towards this the reception at the polyclinic should be able to extend the required assistance to the beneficiary, for identification and authentication.

(vii) The load distribution to respective doctors, pharmacies and laboratories shall be automatically managed by the application deployed at the Polyclinics by the Tenderer. The token generated from the kiosks would act as the queue token and also the medical slip. The size of token should be at least 4”x6”. It should contain the basic details regarding the beneficiary and the waiting serial number at the designated counter/window.
(viii) The patient meets the doctor with the medical examination slip and produces his Smart Card. The doctor inserts the Smart Card into the reader and the records of the beneficiary are fetched from the polyclinic database/data centre. The clinical examinations carried out by the doctor, the medical advice rendered and the medicine prescribed shall be recorded in the central database through the ERP deployed at the polyclinic and shall also be recorded in the smart card. In case the patient is required to be referred, the record of the same shall be endorsed in the smart Card, the Central database, the BPA’s portal and the referred HCO. Referral slip will be generated which will be signed and handed over to the beneficiary.

(ix) The patient goes to the medical store for collection of medicine and produces his smart card, the medicines are issued and record of the medicines is endorsed in the smart card.

(x) In the case of referred patient to HCO’s the patient will report to the referred HCO, there will be one ECHS kiosk deployed at each HCO which will identify and authenticate the beneficiary through Biometric reader on authentication and in the kiosks an integrated camera will capture a real time image of the beneficiary and a referral authentication certificate (RAC) will be generated which will contain the basic details of the beneficiary and the image captured after authentication will be printed on the RAC. This RAC would be required to be enclosed by the HCO’s online for uploading of claims and the hard copy of RAC would be required to be sent to RCs along with the hard copy of the claims.

(xi) The polyclinic will maintain and generate regular reports and returns to its higher headquarters regarding the, patients treated, analysis of diseases, state of medicines etc. For this purpose dashboards will be created and on need to know basis, access as per directions of Central Org shall be provided to the users on the application developed by the BPA.

(f) **Activities at the Station Headquarters.** The medical equipments are issued to the beneficiary by the Stn HQ, hence, an ECHS authentication kiosks will be deployed at each Stn HQ. The authentication kit will authenticate the beneficiary in the similar manner as at the HCOs, the receipt generated after authentication shall have the photograph of the person collecting equipment printed on it. the issue of medical equipment will be endorsed on the smart card, a receipt will be generated by the kiosks which will be signed by the beneficiary and countersigned by the SO ECHS at each Stn HQs. The database shall also be online updated into the Central database and database of the parent polyclinic.
(g) **Data Storage & Transmission.** The database created shall be stored at the following places:-

(i) Data pertaining to the beneficiaries will be stored in the smart card.

(ii) Real time data updation would be carried out on-line into the server of the parent polyclinic.

(iii) Real time updation of data would be done on-line to the Central Data Centre at Central Org ECHS.

(iv) The production data for manufacturing of Smart Cards will also be updated real time and uploaded online into the central database through the leased line circuit established by the Tenderer.

(v) The Tenderer will cater for adequate storage capacity to hold the database and make it available online for the entire duration of the contract.

(vi) The Tenderer will ensure that the data should periodically backed up and global best practices towards data storage and warehousing will be implemented.

(vii) The Tenderer shall not utilize the database or any information related hereof without the permission of the Department.

(viii) The transfer of data from one location to another location will be through leased line/broadband internet circuit and the software at all ends must be capable of receiving data and update their databases.

(h) **Security during transmission.** All data transmission must be done securely and integrity of data must be ensured at all times.

15.3 **CSD SPECIFIC DATA**

(a) **Unit Run Canteens.** Currently there are 3695 Unit Run Canteens (URCs) and 698 extensions, a total of 4393 URCs. All these are automated with the help of CIMS. URCs are categorized into various types as given below:-

<table>
<thead>
<tr>
<th>S No</th>
<th>URC Type</th>
<th>Dependency</th>
<th>Annual Turnover</th>
<th>Unit/Est</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i)</td>
<td>Type ‘A’</td>
<td>Upto 500</td>
<td>1 Cr or less</td>
<td>Minor URC</td>
</tr>
<tr>
<td></td>
<td>Type ‘B’</td>
<td>501 to 1500</td>
<td>1 to 3 Cr</td>
<td>Major URC</td>
</tr>
<tr>
<td>---</td>
<td>------------</td>
<td>-------------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>(ii)</td>
<td>Type ‘C’</td>
<td>1501 to 5000</td>
<td>3 to 8 Cr</td>
<td>Bde &amp; Div HQs/Eqvl</td>
</tr>
<tr>
<td>(iii)</td>
<td>Type ‘D’</td>
<td>5001 to 10000</td>
<td>8 to 15 Cr</td>
<td>Sub Area/Corps &amp; Comd</td>
</tr>
<tr>
<td>(iv)</td>
<td>Type ‘E’</td>
<td>10000 to 15000</td>
<td>15 to 20 Cr</td>
<td>Area HQs / Station</td>
</tr>
<tr>
<td>(v)</td>
<td>Type ‘F’</td>
<td>15000 &amp; above</td>
<td>Above 20 Cr</td>
<td>Army/ Navy/ Air HQs/INCS</td>
</tr>
<tr>
<td>(vi)</td>
<td>Type ‘F’</td>
<td>15000 &amp; above</td>
<td>Above 20 Cr</td>
<td>Army/ Navy/ Air HQs/INCS</td>
</tr>
</tbody>
</table>

(b) Presently, Canteen Inventory Management Software (CIMS) is operational in all URCs. It helps in management of inventory of canteens and also has billing module. Canteen Smart Cards are integrated with CIMS and certain modules of CIMS cannot function unless the Smart Cards are presented. E.g. billing cannot be done unless and until the Smart Card of beneficiary as well as that of operator is inserted into the system. Similarly, there are Installation cards (ISAM) for installing CIMS, Supervisor Card for Inventory management functions. However, all URCs are not networked to each other or to a central data server. CIMS, presently, operates on Windows XP, and Windows Server 2003. The CIMS needs to be upgraded to work on Windows 8 or higher versions and Windows Server 2012 or higher version.

(c) Composite Smart Card to be issued to CSD beneficiaries:-

(i) Grocery cum Liquor cards to serving as well as ex-servicemen.

(ii) Dependent cards: Not-withstanding the entitlement of more dependents in ECHS or Health cards, composite canteen cards for canteen component will only be authorized to maximum two dependents excluding spouse. Entitlement of primary grocery card is sub-allotted in fixed proportions to dependent cards. These cards are linked to each other, are to be issued and activated and if required hot-listed together with primary grocery cards.

(iii) Standalone cards for persons entitled canteen but not other services of health and ECHS: The format of existing cards will continue. Specific categories of persons will continue to operate existing canteen cards and the selected vendor must undertake to provide services and personalize new cards as per existing canteen cards.

(iv) There would be some generic cards called Bronze cards (without personnel details). These are issued to certain institutes like training institutes, hospitals, ASC depots, URCs, DG NCC Camps. Cards for ASC depots, URCs, DG NCC Camps would be allowed to purchase only grocery items up to Rs.5 lakhs in a year.
(v) Plain cards called steel cards only with card no. would be issued to Training Institutes for use by officer cadets/recruits only for duration of the training. This card allows purchase of only grocery items. These will be issued to the trainees on joining and will be withdrawn when they leave the institute.

(d) Mode of Operation in URCs:-

(i) This will be the same as the present operation of Canteen Card.

(ii) Individual will have to go to Points of Service (POS) e.g. billing counter in canteen.

(iii) Billing clerk will insert his operator card in the card reader and keep the system ready for billing. Then, he will insert the customer’s card in the card reader and ask for PIN. After punching the PIN, card can be read by the card reader and billing can be done. for future option Biometric/ PIN reader will be provided.

(iv) Cards will have a ceiling limit for buying grocery in a month depending on the Rank of the cardholder. (This limit may change with time as per policy in vogue).

(v) Similarly for liquor, there would be a ceiling on quantity, depending on rank of the card holder, which can be drawn in a month. An individual can draw up to two months quota of liquor at a time. (This limit may change with time as per policy in vogue).

(e) CIMS and Hardware. Canteen Inventory Management System software will continue to operate as hitherto for and integrated with Health Card and ECHS module. The keys for the Key Management System (KMS) for Canteen Inventory Management Software (CIMS) packages and programming of cards will be handed over to the selected vendor by the existing vendor. The Intellectual Property Rights (IPR) of CIMS will remain with DDGCS office; the vendor will use it for creation of consolidated smart cards, canteen cards and CIMS. Vendor will give a written undertaking that CIMS will not be shared/used by him for any other purpose. CIMS has been upgraded 22 times since 2003 to keep pace with changing requirements. All upgrade versions will be taken over by the selected vendor and handed over by the existing vendor. The vendor must give an undertaking to upgrade CIMS on need based requirement of DDGCS office. More than 4000 URC are fully functional based on CIMS package therefore select vendor will undertake running, maintenance and support to all URC and CIMS from the day contract is signed. Select vendor will also make it compatible with window 8.1 OS/ higher OS which will be provided along with hardware to each URC by vendor.
(i) The current CIMS is developed in VB net and requires Microsoft net framework 1.1. CIMS uses IBM DB2 8.2 database in backend.

(ii) Supporting operating systems are windows 2003/2000 Server and Windows XP SP2.

(iv) CIMS is secured with unique keys stored inside SAM (System Access Module) cards which are authenticated along with pin code for accessing software.

(iv) SAM card is verified at each and every module/step during CIMS functioning.

(v) Different SAM cards are used namely ISAM (Installation System access Module-Installation Key), SSAM (supervisor System Access Module), OSAM (Operator System Access Module) assigned to different canteen staff and administration as per their rights and authorization to operate CIMS.

(vi) Presently CIMS is operating on windows XP; the select vendor shall expedite the migration of CIMS to Windows 8.1/windows 10 / later version free of cost to URCs. Likewise, the vendor shall supply the hardware for all CIMS at all URCs and shall accordingly upgrade the hardware to be compatible with the upgraded version of CIMS with no additional cost.

16. Databases. The composite Smart card and application databases should store, organize and control the data in a unified way for the performance of activities specified in each module. The database should manage basic datasets viz Hospital, ECHS and CSD, independently without interfering others. It should be able to compress, manage, propagate and store the data in the card as well as in the system/ server/ LAN or WAN.

17. Security Features. The system should incorporate a feature to monitor/regulate the users for using the Functionalities & Databases of the application. The system should have the following minimum security features:-

(a) Physical security features must include tamper proof inscriptions on the CSC like name, CSC number. Photograph of the CSC holder should also be tamper proof.

(b) The card operating system and data on the CSC should be secured by 256 bit AES (advanced encryption standards) ISO/IEC18033-3 standards compliant or with latest encryption technology for smart cards available in the market.

(c) The OS and data should be accessible only by HMIS of the services and any un-authorized attempts to read/write data should self delete all the data on the CSC.

(d) The card should have key management system, to ensure authorized access.
(e) Security mechanisms for portioning of data should be implemented within smart card OS as well as in respective applications such that a smart card reader authorized for one application can read only its relevant data and not other modules data (common data will be readable from all authorized terminals).

(f) The vendor will be required to ensure security/vulnerability clearance for hardware and software by an independent third party before they are hosted on the services’ networks. A certificate in this regard would have to be submitted before the system is deployed. In addition, HQ IDS may vet the application software and hardware independently or along with service HQs for any security breaches/other vulnerability. Vendor will have to provide testing servers and client machines along with one of its representative for duration of testing by HQ IDS. In addition, vendor would also be required to provide installation guide.

(g) Adequate security of data should be ensured at all times. No user should have direct access to database and all users should be able to read/write data only through the application software. All kinds of audit trails should be ensured and same should be accessible to the administrator of the system.

(h) The present ECHS software requires internet/public network for operation, Due to this most of ECHS polyclinics are connected via internet but the data of serving personnel cannot be connected and compromised by internet. The vendor will have to provide full proof solution that health and CSD data from Composite Smart card will not be compromised by internet at ECHS terminals.

(j) 15.8 Security during transmission. All data transmitted will be encrypted and the same will be decrypted at the destination. The software should cater for automatic encryption and decryption at senders and receivers end.

(k) Vulnerability testing of the system software as well as the application software is to be carried out by the CERT / government empanelled vendor / or any agency directed by the GOI.

(l) **Information.** The selected vendor may treat all information exchanged as confidential. This shall not, however, preclude disclosure of information exchanged to the competent court of law under their orders when asked for.

(m) **Vendor Staff.** Selected vendor will obtain security clearance for the manpower employed by them from the formation HQ under whose jurisdiction the centres are deployed or co-located. for purpose of obtaining the security clearance, the details of the personnel required to gain access to various centres shall be provided by the select vendor to the respective formation headquarters.

(n) **Application forms.** All filled application forms when verified will be treated as a classified document. Transportation of application forms from one centre to another
will be through the Army Postal Services or through a person authorized by the vendor in a sealed envelope. under no circumstances the application forms will be dispatched through commercial courier services.

(o) **Personalization Centers.** Stringent security measures as per ISO specifications will be established and maintained by selected vendor. the vendor must undertaken to facilitate inspections of DDGCS and rep to personalization centre. All access and exit to personalization centers will be logged and regulated through smart identity cards and biometric based access control systems. Vendor will ensure the security of all data of customers issued with personalized smart card.

(p) **Personalised Smart cards.** Vendor will arrange to handover personalized smart card to the unit run canteens in a sealed box/ package and obtain a receipt for the same from Unit Run Canteens manager.

**Misc Issues**

18. The SCOSTA certification of 128 Kb card from NIC by vendor.

19. The Software platform should be the latest system being offered and cater for future requirements for at least 10 years. The database should permit storage of a large amount of data and fast data retrieval and management.

20. The card and system should be compliant with present legacy systems of ECHS and CSD. The software should be able integrate with present legacy systems i.e. ECHS, CSD, AF MEDNET, different HIS of various hospitals etc.

21. The composite card will be personalized and handed over within 21 days from the date of receipt of application by the vendor.

22. **Software and Hardware training.** Capsule training should be conducted by the vendor for the service personal as System Administrators and Operators.

23. **Warranty.** For at least 5 years and AMC for next 5 years and as per the standard terms of reference. In view of the fast pace of technological advancements, the system should have the capability for maintenance, regular up-gradation and reliable technical support.

24. The procurement philosophy as laid down in DPP 2013 (Defence procurement Procedure 2013) would be followed for project acquisition.

25. Services provided by Existing CSD Vendor to be ensured by Vendor

(a) Establish Central Project Management Centre, Personalization Centre and Helpdesk at New Delhi with communication link to HQ IDS (Med), DDG CS, and Dir ECHS within 30 days from the date of signing of contract.
(b) To establish Regional Project Management Centers and Helpdesks at each Command HQ within 45 days of availability of accommodation or take over existing RPMCs of CSD.

(c) Establish 35 CCTSCs as in given locations However, HQ IDS (Med) may change the locations or add new Collection Cum Technical Support Centers during the implementation of the project.

(d) Deployment of necessary manpower resources at each of above-mentioned centre for implementation of the project.

(e) Installation, maintenance of the Composite Smart Card software and training of all users during the first year of the agreement in consonance with the support package opted by each Unit.

(f) Ensure that no duplicate cards are personalized from different personalization centers by process of networking all personalization centers and establishment of single central server for validating the data.

(g) Ensure that each personalization centre will follow the ISO norms for production, handling and security of Smart Cards.

(h) Execute changes/up gradations in the CIMS and ECHS under the directions of DDGCS and Dir ECHS.

(i) Maintain continuous and effective interaction with the CCO (Central Control Organization) and with HQ Commands for effective implementation of the scheme.

(k) Retention of enrolment and personalized data of customers during the project life cycle.

(l) Maintenance, upkeep, replacement, operation of all deliverables as listed in Annexure “I” attached.

(m) To provide smart card peripherals to all locations in Hospitals, ECHS polyclinics and URCs.

(n) To provide blank printed application form free of cost to users and user sites to be automated and entitled personnel free of cost.

26. **Contract Liability.** The select vendor will also undertake to pay any liability if any which arises due to termination of contract with existing vendor.

27. **Control.** Vendor will have to establish separate division/organization which will be responsible for all CSD/URC matters directly to Canteen services Directorate. on the similar lines separate division/organization for Medical, ECHS may be considered.
Information Sought from Vendor

28. The vendor is to provide the following additional information about the product being offered:-

(a) The detailed Card and hardware specifications of associated equipment to support the application. Vendor will specify the futuristic updating & addition of new features including the customization and integration requirements of the product.

(b) Maintenance philosophy and Training requirements for servers, User machines, Maintenance consoles, Supervisory consoles etc. Vendor should provide alternative options to Web Based Architecture for consideration.

(c) Provide the detailed multilayer security features of the smart card and application to ensure user authenticity & data protection along with associated hardware to support the security features.

(d) Vendor to provide the coordination process between HIMS (for Health and ECHS applications) and CIMS (Canteen Inventory management software) & request grant mechanism between various agencies and modules incorporated in the application.

(e) Complete list of propagation models and various coverage calculations incorporated in the software.

(f) Vendor to provide the list of complete Hardware and Software along with its technical and operational specification including other associated peripheral equipment required to support the project. Specify the bandwidth requirements for the complete application to ensure prescribed quality of service considering the maximum loading.

(g) Provide the license agreements available with vendor for Proprietary and COTS software and also specify the Licensing model of the application being offered.
Annexure-II
(Refers to Para 6(a) of RFI)

INFORMATION PROFORMA
(INDIAN VENDORS)

1. Name of the Vendor/Company/Firm.

____________________________________________________________________________________
(Company profile, in brief, to be attached)

2. Type (Tick the relevant category).

Original Equipment Manufacturer (OEM) Yes/No
Authorized Vendor of foreign Firm Yes/No (attach details, if yes)
Others (give specific details)

3. Contact Details.
Postal Address: __________________________
City: __________________ State: __________________
Pin Code: _______________ Tele: __________________
Fax: __________________ URL/Web Site: _____________________

4. Local Branch/Liaison Office in Delhi (if any).
Name & Address: __________________________
Pin code: _______________ Tel: _______________ Fax: ________________________

5. Financial Details.
   (a) Category of Industry (Large/medium/small Scale) _____________________________
   (b) Annual turnover: _________________________ (in INR)
   (c) Number of employees in firm: _____________________________
   (d) Details of manufacturing infrastructure: _____________________________
   (e) Earlier contracts with Indian Ministry of Defence/Government agencies:

<table>
<thead>
<tr>
<th>Contract Number</th>
<th>Equipment</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Name of Agency</th>
<th>Certification</th>
<th>Applicable from (Date &amp; Year)</th>
<th>Valid till (Date &amp; Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7. Details of Registration.

<table>
<thead>
<tr>
<th>Agency</th>
<th>Registration No.</th>
<th>Validity (Date)</th>
<th>Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DGS&amp;D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DGQA/DGAQA/DGNAI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OFB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DRDO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other Government Agency</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. Membership of FICCI/ASSOCHAM/CII or other Industrial Associations.

<table>
<thead>
<tr>
<th>Name of Organization</th>
<th>Membership Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Equipment/Product Profile (to be submitted for each product separately)

(a) Name of Product: ____________________________________________
(Should be given category wise for e.g. all products under night vision devices to be mentioned together)
(b) Description (attach technical literature): _______________________
(c) Whether OEM or Integrator: ______________________________________
(d) Name and address of foreign collaborator (if any): ________________
(e) Industrial License Number: ____________________________________
(f) Indigenous component of the product (in percentage): _______________
(g) Status (in service /design & development stage): ________________
(h) Production capacity per annum: _________________________________
(j) Countries/agencies where equipment supplied earlier (give details of qty supplied): ____________________________________________
(k) Estimated price of the equipment: _______________________________

10. Alternatives for meeting the objectives of the equipment set forth in the RFI.

11. Any other relevant information: _________________________________

12. Declaration. It is certified that the above information is true and any changes will be intimated within five (05) working days of occurrence.

(Authorized Signatory)
INFORMATION PROFORMA (FOREIGN VENDORS)

1. Name of the Vendor/Company/Firm.
(Company profile, in brief, to be attached)

2. Type (Tick the relevant category).
   - Original Equipment Manufacturer (OEM): Yes/No
   - Authorized Vendor of foreign Firm: Yes/No (Details of registration to be provided)
   - Others (give specific details)
   - Government sponsored Export Agency: Yes/No (attach details)

3. Contact Details.
   - Postal Address:
   - City:
   - Province:
   - Country:
   - Pin/Zip Code:
   - Tele:
   - Fax:
   - URL/Web Site:

4. Local Branch/Liaison Office/Authorized Representatives, in India (if any).
   - Name & Address:
   - City:
   - Province:
   - Country:
   - Pin/Zip Code:
   - Tele:
   - Fax:

5. Financial Details.
   - Annual turnover: _______________________ USD
   - Number of employees in firm: ______________________
   - Details of manufacturing infrastructure: ______________________
   - Earlier contracts with Indian Ministry of Defence/Government agencies:

<table>
<thead>
<tr>
<th>Agency</th>
<th>Contract Number</th>
<th>Equipment</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. **Certification by Quality Assurance Organization.**

<table>
<thead>
<tr>
<th>Name of Agency</th>
<th>Certification</th>
<th>Applicable from (Date &amp; Year)</th>
<th>Valid till (Date &amp; Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Equipment/Product Profile (to be submitted for each product separately)

(a) Name of Product: ____________________________
(Should be given category wise for e.g. all products under night vision devices to be mentioned together)

(b) Description (attach technical literature): ____________________________

(c) Whether OEM or Integrator: ____________________________

(d) Status (in service/design & development stage): ____________________________

(e) Production capacity per annum: ____________________________

(f) Countries where equipment is in service ____________________________

(g) Whether export clearance is required from respective Government: _____

(h) Any collaboration/joint venture/co production/ authorized dealer with Indian industry (give details):
    Name & Address: ____________________________
    Tel: __________________ Fax: __________________

(j) Estimated price of the equipment ____________________________

8. Alternatives for meeting the objectives of the equipment set forth in the RFI.

9. Any other relevant information. ____________________________

10. Declaration. It is certified that the above information is true and any changes will be intimated within five (05) working days of occurrence.

    (Authorized Signatory)