रक्षा लेखा प्रधान नियंत्रक (अफसर) कार्यालय
गोलीबार मैदान, पुणे – 411001
Principal Controller of Defence Accounts (Officers)
Golibar Maidan, Pune - 411001
दूरभाष/ **TEL: 020 –26401144** फैक्स / **FAX: 020 – 26453446**

No.EDP/85/ Website/IV Date 02/09/2022

To
M/s Maple Cloud Technologies
#S01, 2nd Floor, B-46,
Sector -63,
Noida - 201301

Sub:-Website & Web application audit.
Ref:- Your quotation dated 30/07/2022.
*****

Dear Sir,

This has reference to your quotation dated 30/07/2022 regarding Website and Web Application Audit. We are pleased to inform you that this office has accepted your quotation for carrying out the above job as per CERT-In guidelines at a total cost of Rs.[illegible] only) as per terms and conditions enclosed in Annexure –'A'.

S No	Description	Cost in Rupees Rs.
1	Audit Cost per audit including reaudit	[illegible]
2	Taxes & Levies (GST 18%)	[illegible]
3	Total Cost	[illegible]
	(Rs [illegible] only)	

2. Scope of Audit: The scope of audit is as per Annexure-'B' and also if any, add-on feature available on the website.

3 The above job may please be completed as early as possible including submission of audit report thereof.

4 A pre-receipted invoice in triplicate (original copy affixed with a revenue stamp) duly supported with a copy of accepted service report may be submitted to this office for payment after successful completion of job.

Sd/-
(J N Tulekar)
Sr. Accounts Officer (EDP)

\\192.168.16.26\vinadmin_old\supplyorder\web site\WO web cum Application audit 0822.doc

Annexure 'A'

Schedule of Requirements:
The details of scope and quality of services are provided in succeeding paragraphs:

1. Scope of Work/Service:
The scope of audit includes audit of complete PCDA(O), Pune website viz. https://pcdaopune.gov.in and website applications. Details as per Annexure-'B' and also if any, add-on feature available on the website.

2. Terms and conditions:
The following terms and conditions may please be adhered to :

2.1 **Timeframe of the deliverables:**
a. Your firm will be required to start the project within 15 days from the date of placing the order for the audit.
b. The audit should be completed within 60 days of receipt of Work Order. However, intermediate report should be submitted within 30 days. The EDP team of PCDA(O) will give feedback on the intermediate report within 07 days. Such feedback should be addressed in the final report.
c. All the draft reports of the agreed deliverables should be submitted by the firm within 30 days of the commencement of the audit.
d. After patching up the vulnerabilities, if any by website developer firm, the re-audit should be done within 7 days of intimation by this office.
E .Audit of the website and web application should be done till all vulnerabilities are successfully rectified.
f. The audit, as mentioned above, has to be completed in time. It is expected that, if required, the successful bidder may deploy multiple teams to complete the audit projects within given time frame.

3.2 **Payment terms**: The payment will be made on after successful completion of audit and submission of final report thereof.

3.3 **Security factor:** Your firm should furnish an undertaking that it would abide by Government directives on security issues for IT contracts, issued from time to time. Accordingly, your firm will not disclose any information related to database being maintained in this office to any outside person nor shall take them out in any form without the permission of the system administrator/Project Leader from PCDA (O). Your firm should also give an undertaking that it would not use the source code for any other purpose nor shall share with any outsider under any circumstances. The absolute ownership of the source code will be that of PCDA(O) only.

3.4 **Prohibition:** Prohibition against use of PCDA(O) name without prior written permission for Publicity Purpose. The parties participating/ contributing in this contract jointly/ independently shall not use PCDAO(O) name / logo for any publicity purpose through any public media viz. press, radio, television, etc., without prior written approval.

3.5 **Submission of Audit report**: The audit report may be submitted to this office within three days after completion of security Audit. Delay in submission of the Report will treat as defective service and penalty will be as per para 8 of Part III.

.

Part III - Standard Conditions Of Contract

1. **Law:** The contract shall be considered and made in accordance with the laws of the Republic of India. The contract shall be governed by and interpreted in accordance with the laws of the Republic of India.

2. **Effective date of the contract**: The contract shall come into effect on the date of signatures of both the parties on the contract (Effective Date) and shall remain valid until the completion of the obligations of the parties under the contract. The performance of the services shall commence from the effective date of the contract.

3. **Arbitration:** All disputes or differences arising out of or in connection with the contract shall be settled by bilateral discussions. Any dispute, disagreement or question arising out of or relating to the contract or relating to construction or performance, which cannot be settled amicably, may be resolved through arbitration.

4. **Penalty for use of Undue influence** : The Vendor undertakes that he has not given, offered or promised to give, directly or indirectly, any gift, consideration, reward, commission, fees, brokerage or inducement to any person in service of the Buyer or otherwise in procuring the Work Order or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of the present Work Order or any other Work Order with the Government of India for showing or forbearing to show favour or disfavour to any person in relation to the present Work Order or any other Work Order with the Government of India. Any breach of the aforesaid undertaking by the Vendor or any one employed by him or acting on his behalf (whether with or without the knowledge of the Vendor) or the commission of any offers by the Vendor or anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the Buyer to cancel the Work Order and all or any other Work Orders with the Vendor and recover from the Vendor the amount of any loss arising from such cancellation. A decision of the Buyer or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Vendor. Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the Vendor towards any Officer/employee of the Buyer or to any other person in a position to influence any Officer/employee of the Buyer for showing any favour in relation to this or any other Work Order, shall render the Vendor to such liability/ penalty as the Buyer may deem proper, including but not limited to termination of the Work Order, imposition of penal damages and refund of the amounts paid by the Buyer.

5. **Agents / Agency Commission** : The Vendor confirms and declares to the Buyer that the Vendor is the original provider of the services referred to in this Work Order and has not engaged any individual or firm, whether Indian or foreign whatsoever, to intercede, facilitate or in any way to recommend to the Government of India or any of its functionaries, whether officially or unofficially, to the award of the Work Order to

the Vendor; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Vendor agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in any way incorrect or if at a later stage it is discovered by the Buyer that the Vendor has engaged any such individual/firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this Work Order, the Vendors will be liable to refund that amount to the Buyer. The Vendor will also be debarred from entering into any work, Work Order with the Government of India for a minimum period of five years. The Buyer will also have right to consider cancellation of the Work Order either wholly or in part, without any entitlement or compensation to the Vendor who shall in such an event be liable to refund all payments made by the Buyer in terms of the Work Order along with interest at the rate of 2% per annum above LIBOR rate. The Buyer will also have the right to recover any such amount from any Work Orders concluded earlier with the Government of India.

6. **Access to Books of Accounts:** In case it is found to the satisfaction of the Buyer that the Vendor has engaged an Agent or paid commissions or influenced any person to obtain the work order as described in clauses relating to Agents/Agency Commission and penalty for use of undue influence, the Vendor, on a specific request of the Buyer, shall provide necessary information/ inspection of the relevant financial documents/ information.

7. **Non-disclosure of contract documents:** Except with the written consent of the Buyer, Vendor/other party shall not disclose the contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party. As the data consists of personal details of defence personnel, it is necessary to keep the working tool and hardware within the Office premises and the vendor or his representatives/ employees are not allowed to use the same outside this Office. The representatives of the Vendor will ensure due confidentiality in this regard.

8. **Liquidated damages:** In the event of the Vendor's failure to submit the Bank Guarantee, Documents and Codes the Buyer may, at his discretion, withhold any payment until the completion of the contract. The Buyer may also deduct from the Vendor as agreed, Liquidated Damages to the sum of 0.5% of the contract price of the delayed/undelivered services mentioned above for every week of delay or part of a week, subject to the maximum value of the Liquidated Damages being not higher than 10% of the value of delayed services. The LD cannot exceed the amount stipulated in the contract.

If the delay is longer than Ten weeks, the buyer shall, except as provided hereinafter, be entitled to cancel the order in full or in part at their sole discretion without any financial repercussions on Govt. of India.

9. **Termination of the contract:** The Buyer shall have the right to terminate this contract in part or in full in any of the following cases:-

(a) The delivery of the services is delayed for causes not attributable to Force Majeure for more than 3 days after the scheduled date of delivery.

(b) The Vendor is declared bankrupt or becomes insolvent.

(c) The delivery of services is delayed due to causes of Force Majeure by more than three (3) months provided Force Majeure clause is included in work order.

(d) The Buyer has noticed that the Vendor has utilised the services of any agent in getting this contract and paid any commission to such individual/company etc.

(e) As per decision of the Arbitration Tribunal.

10. **Notices:** Any notice required or permitted by the contract shall be written in the English language and may be delivered personally or may be sent by e-mail/ FAX or registered e-mail, addressed to the last known address of the party to whom it is sent.

11. **Transfer and sub-letting:** The Vendor has no right to give, bargain, sell, assign or sublet or otherwise dispose of the contract or any part thereof, as well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.

12. **Patents and Other Industrial Property Rights:** The prices stated in the present contract shall be deemed to include all amounts payable for the use of patents, copyrights, registered charges, trademarks and payments for any other industrial property rights. The Vendor shall indemnify the Buyer against all claims from a third party at any time on account of the infringement of any or all the rights mentioned in the previous paragraphs, whether such claims arise in respect of service delivery. The Vendor shall be responsible for the completion of the contract, irrespective of the fact of infringement of any or all the rights mentioned above.

13. **Intellectual Proprietary Rights (IPR**): Any intellectual Proprietary owned/ purchased by vendor prior to the execution of this Agreement and used by vendor in the performance of its obligation under this Agreement shall remain the exclusive property of vendor. Any intellectual property owned/purchased by PCDA(O), Pune prior to the execution of this Agreement and used by PCDA(O), Pune in the performance of its obligation under this Agreement shall remain the exclusive property of PCDA(O), Pune. The developed application software will be exclusive property of PCDA(O), Pune only.

14**. Amendments:** No provision of present Contract shall be changed or modified in any way (including this provision) either in whole or in part except by an instrument in writing made after the date of this Contract and signed on behalf of both the parties and which expressly states to amend the present Contract.

15. **Taxes and Duties**: Any change in any tax upward/downward as a result of any statutory variation taking place within contract terms shall be allowed to the extent of actual quantum of such tax paid by the supplier. Similarly, in case of downward revision in any tax, the actual quantum of reduction of such duty/tax shall be reimbursed to the Buyer by the Vendor.

Part IV - Special Conditions Of Contract

1. **Performance Guarantee/ Indemnity Bond**:

a) The entire contract period will be covered by Performance Bank Guarantee equal to the 10% value of the contract.
b) B.G. from SBI or other Public Sector Banks or ICICI Bank Ltd or HDFC bank Ltd or AXIS Bank Ltd only be accepted on a stamp paper of the value not less than Rs. 50.00
c) The Performance Bank Guarantee should have a validity period of 15 months.

2**. Payment Terms:**

a) The payment will be made on after successful completion of audit and submission of final report thereof.

b) It is mandatory to obtain a user acceptance certificate towards delivery and inspection of stipulated deliverables conveying satisfaction of the user duly signed by the Officer-in-Charge of EDP Section.

c) Certificate so obtained must be enclosed along with the bills for disbursement of the payment.

d) Any penalty imposed as per the terms and conditions of the contract shall be deducted from the amount due for payment.

e) E-payment will be made through SBI-CMP into the Bank Account of the vendor. Therefore, it is mandatory for the vendor to indicate their Bank Account Number and other relevant details like Name of the Account Holder, Name of the Bank & Address & IFSC Code etc.
f) If any discrepancy is found in amount quoted in words and figures, then the amount mentioned in words will be treated as correct and final.

3.**Force Majeure:** Should any Force Majeure circumstances arise, each of the contracting party shall be excused for the non-fulfillment or for the delayed fulfillment of any of its contractual obligations, if the affected party within 10 days of its occurrence informs the other party in writing. Force Majeure shall mean fires, floods, natural disasters or other acts, that are unanticipated or unforeseeable, and not brought about at the instance of the party claiming to be affected by such event, or which, if anticipated or foreseeable, could not be avoided or provided for, and which has caused the non-performance or delay in performance, such as war, turmoil, strikes, sabotage, explosions, quarantine restriction beyond the control of either party. A party claiming Force Majeure shall exercise reasonable diligence to seek to overcome the Force Majeure event and to mitigate the effects thereof on the performance of its obligations under this contract.

4. **Specifications**: The Vendor guarantees to meet the specifications as per Part-II

of this Contract and to incorporate the modifications to the existing design configuration to meet the specific requirement of the Buyer Services as per modifications/requirements recommended. The Vendor, in consultation with the Buyer, may carry out technical upgradation/ alterations in the design, coding and specifications due to change in logic, coding, procedures or obsolescence. This will, however, not in any way, adversely affect the end specifications and desired output of the software/ website. Changes in technical details, logic, coding, design techniques along with necessary changes as a result of upgradation/ alterations will be provided to the Buyer free of cost within stipulated time frame of affecting such upgradation/ alterations.

5. **Audit:** The audit should be completed within 60 days of receipt of Work Order. However, intermediate report should be submitted within 30 days.

6. **Risk and Expense clause**:

a. Should the service or any instalment thereof not be delivered with the time or time specified in the contract documents, or if defective delivery is made in respect of the services or any instalment thereof, the Buyer shall after granting the Vendor 1(one) week to cure the breach, be at liberty, without prejudice to the right to recover liquidated damages as a remedy for breach of contract, to declare the contract as cancelled either wholly or to the extent of such default.

b. Should the services or any instalment thereof not perform in accordance with the specifications / parameters provided by the Vendor during the testing stage, the Buyer shall be at liberty, without prejudice to any other remedies for breach of contract, to cancel the contract wholly or to the extent of such default.

c. In case of a service breach that was not remedied within One(1) week, the Buyer shall, having given the right of first refusal to the Vendor be at liberty to purchase, or procure from any other source as he thinks fit services of the same or similar description to make good:-

i. Such default.

ii. In the event of the contract being wholly terminated the balance of the services remaining to be delivered there under.

d. Any excess of the purchase price, or value of any services procured from any other supplier as the case may be, over the contract price appropriate to such default or balance shall be recoverable from the Vendor.

Annexure –'B'

Scope of Contract

Your firm would be expected to perform the following tasks:

1. Application Security Testing, re-testing to confirm closure of Vulnerability.

2. **Web Application Test:**

It would be expected to perform the following tasks for Website and the web application Security to analyze and review the website/application security .The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in website through Internet Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security of the website.

The identified solutions should be very specific and objective. Vague language should be avoided in the same. The solution proposed shall refer to specific application code and database. Your firm will also be expected to propose a risk mitigation strategy as well as give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment. The website and Web-application should be audited as per the Industry Standards and also as per the OWASP (Open Web Application Security Project) model. Such should be included in intermediate report proposal. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented.

The scope of the proposed audit tasks is given below. The audit firm will be required to prepare the checklist/reports.

3. Web Security Audit/ Assessment:

Check various web attacks and web applications for web attacks. The various checks /attacks /Vulnerabilities should at least cover the following or any type of attacks, which are vulnerable to the website/Web-application.

- Vulnerabilities to SQL Injections
- CRLF injections
- Directory Traversal
- Authentication hacking/attacks
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Exploitable hacking vulnerable
- Web server information security
- Cross site scripting
- PHP remote scripts vulnerability
- HTTP Injection

- Phishing a website
- Buffer Overflows, Invalid inputs, insecure storage etc .
- Other any attacks, not covered by above mentioned list, which are vulnerable to the website and web applications

The Top 10 Web application vulnerabilities (as per OWASP) (Open Web Application Security Program), which are given below, should be checked up for the given web applications at minimum and separate annexure in detail should be there in report.

a	Cross Site Scripting(XSS)	XSS occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, insert hostile content, conduct phishing attacks and take over the user's browser using scripting malware.
b	Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
c	Insecure Remote File Inclusion	Code vulnerable to remote file inclusion allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise
d	Insecure Direct Object reference	A direct object reference occurs when a developer expose a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attacker can manipulate those references to access other objects without authorization
e	Cross site request Forgery (CSRF)	On completion of audit and application patching the vendor will check the impact of patching for availability and integrity. The sample functionality check points made during the task2 stage will be used to verify any functionality issue. This test report will be submitted to MPCB.
f	Information leakage and Improper Error handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use the weakness to violate privacy, or conduct further attacks
g	Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume user's identity.
h	Insecure Cryptographic	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use

	Storage	weakly protected data to conduct identity theft and other crimes, such as credit card fraud
i	Insecure communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
j	Failure to Restrict URL Access	Frequently, the only protection for sensitive areas of an application is links or URLs are not presented to authorized users. Attackers can use this weakness to access and perform unauthorized operations.

The applications have to be tested for Functional application security as well in an objective manner.

4. **Re-Audit**: Your firm will be responsible to provide a detailed recommendation report for vulnerabilities observed.

5. **Re, Re-Audit**: If vulnerabilities are observed from the re-audit, this cycle will continue till all the vulnerabilities have been mitigated.

6. **Deliverables and Audit Reports**:

General: The responsibility of submitting all reports is attributed to your firm. The signature on the reports/certificate(s) submitted by the auditor, CISSP, will be on his firm's letterhead.

The vendor will be required to submit the following documents after the application audit:

a. A detailed and summary report will be submitted detailing the discovered vulnerabilities, the impact of the vulnerability with associated risk levels and recommendations for risk mitigations. The detailed report will also give the steps/methods used to establish the vulnerability along with screen-shots.

b. For a given vulnerability all possible links affected in the application will be specified.

c. For re-audit reports, the previous level summary report needs to be updated, giving the audit level and the updated status of the vulnerability (open/closed). In the event a new vulnerability is determined at a re-audit level a new summary table for that level will be made and in the detailed report the auditor will specify the reason for finding vulnerability at a re-audit stage.

d. The auditing vendor will submit the audit report at every stage to PCDA(O). The report may be mailed to PCDA(O). This is a measurable parameter for the project progress.

7. Audit Report:

The Website security audit report is a key audit output and must contain the following:

a. Identification of auditee(Address & contact information)
b. Dates and Location(s) of audit
c. Terms of reference (as agreed between the auditee and auditor), including the standard for Audit, if any
d. Audit plan
e. Explicit reference to key auditee organisation documents (by date or version) including policy and procedure documents
f. Additional mandatory or voluntary standards or regulations applicable to the auditee.
g. Standards followed
h. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
i. Tools used
ii. List of vulnerabilities identified.
iii. Description of vulnerability
iv. Risk rating or severity of vulnerability
v. Test cases used for assessing the vulnerabilities
vi. Illustration if the test cases to provide the vulnerability
vii. Applicable screen dumps
i. Analysis of vulnerabilities and issues of concern
j. Recommendations for action
k. .Personnel involved in the audit, including identification of any trainees The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.
l. The successful bidder must also follows the guidelines of National Informatics Center (NIC) for website security Audit and submit the Audit report as per the format mentioned in guidelines.

8. Issuance of "Fit for Hosting" certificate as per NIC guidelines.

The deliverable is a secure application fit for hosting at NIC, as per NIC guidelines without affecting the functionality of the original application.

Sd/-
(J N Tulekar)
Sr Accounts Officer(EDP)

A. I. Login utility to around 60,000 users and respective passwords.

II. For each user, the following facility to be provided:

a. Password
   i. Change password
   ii. Forgot password hint question
   iii. Application format utility if forgot password hint question and answer is also forgotten.

b. Uploading
   i. Uploading DSOP Fund withdrawal claim (.pdf format) by user
   ii. Upload CEA and other Miscellaneous Claims by users
   ii. Upload grievances
   iii. Upload saving proof (.pdf format) for IT purpose
   iv. Uploading of TA/DA Claims online
   v. Uploading of Change in DSOP Subscription.
   vi. Uploading of DSOP nomination form.

c. Download .pdf outputs
   i. Monthly Statement of Accounts
   ii. Annual DSOP Fund Statement for last 2 years
   iii. Form-16 for the last 2 years.
   iv. Intimation/ Rejection Memos if any.

d. View information
   i. Position of outstanding TA/DA advances
   ii. Passing Memo of Ledger Wing Claims
   iii. Status of both Ledger Wing & T Wing Claims
   v. Passing Memo of TA/DA Claims
   vi. Cheque Payment details.
   vii. Rejection details of Requisitions & Claims.
   viii. Status of DSOP Fund Claims
   ix. Status of advance of LTC leave encashment claim.

e. Generation of Dak-id for all type of submission by users.

f. High Security at multiple levels of the system which facilitates powerful system monitoring and administration.

g. Creation of user constraints (roles and permissions) and deciding scope for them e.g. list, a given module or whole system.

h. Maintains log details for every transaction performed in the system.

i. Access restricted to authorized user and transaction controls like (Create, Edit, View, Approve etc.)
j. Authentication for Users ID & Password and Encryption for password using encryption techniques.
k. Online grievance redressal system i.e Users can write their grievances which will be replied online through a reply box.
l. Automated generation of payment intimation to concerned log-in users through e-mail (60000 users).

B. Login utility for AAO BSOs
   a. Around 500 users and respective passwords
   b. change passwords
   c. Upload text file by users.
   d. Download rejection/ Intimation memo.

C. Login utility for veteran Cell, HQSC which will be IP based.
   a. receiving query, give ID and download
   b. uploading reply against each id.

D. Login utility for Veteran Cell, AHQ - IP based (a) & (b) as above.

E. Website Admin- Development of periodic upload/download utilities for web admin.
   a. Adding new user and generating one time username and password; removing existing users.
   b. Updating username & password
   c. Updating static information
   d. Uploading (.pdf) replies to grievances received through Veteran Cell. DSOP Fund Statement, O/S T Wing Advances, Passing memos of T Wing and LW Claims.
   e. Downloading grievances, received from Veteran Cell and Serving Officers, Files received from AAO(BSOs), DSOP Fund Withdrawal Claim,TA/DA claims, CEA Claim, Saving Certificate for IT purpose.
   f. Updating fix info for all log in utilities.

F. Development of pages in Hindi Devnagari script. (pages which are meant for viewing by users).

G. Information display & links on Home Page.

H. Website Security Architecture Management:

The portal will have a secure login for admin user as well as other users. Captcha image will be provided for prevention of email & password hacking. Audit Trail will be implemented in the proposed solution, so that the admin can check the successful & unsuccessful login attempts with time & IP address. The website will be protected from virus with the help of the firewall. The security of the website will be audited by the cert-in empanelled certificate. There will be analysis and reporting tools to track the portal system usage.

I. Any other activity/ utility required for all utilities/ services mentioned at Sl No. A to H.