



ISO 9001-2000,
ISO 140 01-1996
OHSAS 18001-1999



नॉर्थ ईस्टर्न इलेक्ट्रिक पावर कॉर्पोरेशन लिमिटेड

(भारत सरकार का उद्यम)

NORTH EASTERN ELECTRIC POWER CORPORATION LTD

(A GOVT. OF INDIA ENTERPRISE)

CIN U40101ML1976GOI001658

OFFICE OF THE EXECUTIVE DIRECTOR (CONTRACTS & PROCUREMENT)

BROOKLAND COMPOUND::LOWER NEW COLONY

SHILLONG-793003, MEGHALAYA

Website: www.neepco.co.in Email: contract_neepco@yahoo.com

PHONE: +91-364 2225547 FAX: +91 364-2222578

NEEPCO/QP/C&P/F/E/IT Audit/2050/Vol-I/ 1394

dated 02/01/2018

To

M/s AKS Information Technology Services Pvt. Ltd.
E-52, First Floor, Sector-3, Noida-201301

Sub: Letter of Intent to award the contract for IT Security Audit of NEEPCO

- Ref:
1. Our NIB No. 248 dtd. 16/08/17
 2. Your online bid and bid in e-RA dtd. 04/12/17
 3. Our letter No. NEEPCO/QP/C&P/F/E/IT Audit/2050/Vol-I/1225 dtd. 08/12/17
 4. Your letter No. AKSIT/NEEPCO/2017/02 dtd. 08/12/17

Dear Sirs

With reference to the above and you being an MSE bidder with NSIC Registration No. NSIC/GP/NOI/2015/0017073, we are pleased to place this Letter of Intent (LOI) for award of the works for IT Security Audit of NEEPCO as per the Terms and Condition given hereunder:

1. SCOPE:

(a) **Vulnerability Assessment (VA) of IT hosts/devices listed at Annexure 1 Sl. 1**

(i) **Vulnerability Assessment and Penetration Testing**

Perform black box (without user credentials) vulnerability assessment and penetration testing (VAPT) of the systems/devices using both automated and manual techniques. The manual assessment will be performed to remove false positives and identify vulnerabilities not reported by automated tool. This will be done without using any user credentials or in non-privileged mode.

(ii) **Configuration review of IT hosts/devices**

1. Perform Configuration review of the systems/devices to identify any potential security weaknesses.
2. Collect Information about the current security configuration of the hosts/ devices by running script/system commands with highest privilege or through examination of System Configuration files. The scripts/command details will be provided by the Auditor.
3. Running of the scripts/commands or copying of the configuration files will be done by the respective system administrators of the client organization (under the



ISO 9001-2000,
ISO 140 01-1996
OHSAS 18001-1999



नॉर्थ ईस्टर्न इलेक्ट्रिक पावर कॉर्पोरेशन लिमिटेड

(भारत सरकार का उद्यम)

**NORTH EASTERN ELECTRIC POWER CORPORATION LTD
(A GOVT. OF INDIA ENTERPRISE)**

CIN U40101ML1976GOI001658

**OFFICE OF THE EXECUTIVE DIRECTOR (CONTRACTS & PROCUREMENT)
BROOKLAND COMPOUND::LOWER NEW COLONY**

SHILLONG-793003, MEGHALAYA

Website: www.neepco.co.in Email: contract_neepco@yahoo.com

PHONE: +91-364 2225547 FAX: +91 364-222578

supervision of the Auditor) and the output or the copy of the configuration files will be submitted to the Auditor for analysis and interpretation.

(b) Security Audit of IT Applications and Web Applications listed at Annexure 1 Sl. 2:

It includes Application Security and Website Assessment (including database) to ensure that the applications are secure from both external and internal attacks. The assessment will be carried out based on OWASP Top 10 and SANS Top 20 vulnerabilities. The assessment will include, but not limited to, the following areas:

1. **Identification of security vulnerabilities:** Assessment of the host centric database application Matfin to identify vulnerabilities like cross-site scripting, SQL injection, session hijacking, privilege escalation, data leakage, improper database settings, etc.
2. **User access management:** Review the process followed for granting, revocation, transfer and deletion of application access.
3. **Super User process management:** Review process followed for creation of Super User such as System Administrator, Database Administrator (DBA), etc.
4. **Security policy compliance:** Review application and website compliance to security policy such as password policy, audit trail, logging and monitoring.
5. **Change Control:** Review the process followed by the development team to manage and implement changes in the application.
6. **Incident and Patch Management:** Review the process followed for managing Incident and patches for the various changes and upgrades carried out in the application.
7. **Misconfigurations:** Assess and review the configuration settings of the applications and associated databases.

(c) Security Assessment of IT Operations and Processes at NEEPCO Corporate Office, Shillong

1. **Review of Information Security Policies and Procedures:** The existing information security policies and procedures should be reviewed in accordance with the ISO 27000 series of international information security standards
2. **BCP/DR assessment and readiness review:** Review the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP), if any, and associated processes for the existing critical infrastructure.



ISO 9001-2000,
ISO 140 01-1996
OHSAS 18001-1999



नॉर्थ ईस्टर्न इलेक्ट्रिक पावर कॉर्पोरेशन लिमिटेड

(भारत सरकार का उद्यम)

NORTH EASTERN ELECTRIC POWER CORPORATION LTD

(A GOVT. OF INDIA ENTERPRISE)

CIN U40101ML1976GOI001658

OFFICE OF THE EXECUTIVE DIRECTOR (CONTRACTS & PROCUREMENT)

BROOKLAND COMPOUND::LOWER NEW COLONY

SHILLONG-793003, MEGHALAYA

Website: www.neepco.co.in Email: contract.neepco@yahoo.com

PHONE: +91-364 2225547 FAX: +91 364-2222578

(Note : The preparation of BCP / DR plan is not covered as part of the scope of work.)

3. **Incident and Patch Management:** Review the process followed for managing and reporting Incident and patches for the various changes carried out in the IT infrastructure / application.
4. **User Access Management:** Review process followed for user access management, application role assignment, privilege user access, account and password sharing at sites.
5. **Change Control:** Review the process followed to manage and implement changes at the IT infrastructure and applications.
6. **User awareness and compliance:** Perform user security awareness assessment by conducting interviews of the users. This review will include user awareness on security policy, password management, account management and incident reporting.
7. The physical security arrangement of the major IT installations and equipment must be audited.

The mode of conducting the above assessments will be primarily On-site.

2. **CONTRACT VALUE:** The total contract value for the entire scope of work shall be Rs. 3,65,000.00 (Rupees Three lakh Sixty Five Six thousand) only, inclusive of GST as per the break-up of Price Schedules A and B attached.

The prices shall remain FIRM during the entire contract period.

3. **COMPLETION TIME:** 3 (three) months from the date of issue of LOI for the work.
4. **CONTRACT PERFORMANCE GUARANTEE:** Within 15(Fifteen) days from the date of issue of Letter of Intent, the Contractor shall furnish a Bank Guarantee in prescribed format (as provided in the bid document Sec IX), for an amount equal to 10 (ten) percent of the Contract value by way of Guarantee for the due and faithful performance of the Agreement and for the due and faithful performance of the **Letter of Intent** along with the other terms and conditions agreed to. The Bank Guarantee shall be initially valid for such period to cover 90 (ninety) days after the completion period of the contract as per Agreement.

5. **ENGINEER IN CHARGE :**



ISO 9001-2000,
ISO 140 01-1996
OHSAS 18001-1999



नॉर्थ ईस्टर्न इलेक्ट्रिक पावर कॉर्पोरेशन लिमिटेड

(भारत सरकार का उद्यम)

**NORTH EASTERN ELECTRIC POWER CORPORATION LTD
(A GOVT. OF INDIA ENTERPRISE)**

CIN U40101ML1976GOI001658

**OFFICE OF THE EXECUTIVE DIRECTOR (CONTRACTS & PROCUREMENT)
BROOKLAND COMPOUND::LOWER NEW COLONY**

SHILLONG-793003, MEGHALAYA

Website: www.neepco.co.in Email: contract_neepco@yahoo.com

PHONE: +91-364 2225547 FAX: +91 364-2222578

Till issue of Letter of Intent, subsequent detailed Order on behalf of the Corporation and acceptance of CPG:

The General Manager i/c C&P, NEEPCO, Shillong

Phone no. 0364-2225547

Fax no. 0364 2222578

e-mail: contract_neepco@yahoo.com

After issue of Letter of Intent:

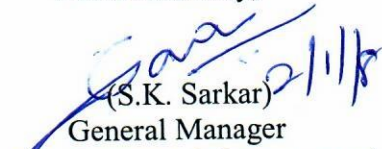
The DGM(IT), NEEPCO, Lower New Colony, Shillong-793003 or his authorized representatives.

6. **DETAILED ORDER:** The detailed order will be issued on unconditional acceptance of the Letter of Intent.
7. **OTHER TERMS AND CONDITIONS:** The terms and conditions of Notice Inviting Bids and the Bid Documents and amendments thereof issued from time to time, if any, shall prevail for execution and completion of the entire scope of the Contract in all respects.

The Contractor shall give unconditional acceptance of the LOI within 3(three) days from the date of issue of the LOI.

Thanking you,

Yours faithfully,


(S.K. Sarkar)
General Manager
i/c Contract & Procurement
NEEPCO Ltd., Shillong.

1. List of Active Hosts /Devices for vulnerability assessment

Annexure-I

Sl. No.	Hosts /Devices	Make & Model	Qty.
1	Firewall	Cyberoam CR1500ia	1
2	-do-	Cyberoam CR50iNG	1
3	Firewall Analyser	Cyberoam CR-iVU100NR/SCB1802	1
4	Layer 3 Switch	Extreme	7
5	Core Switch	Extreme & Black Diamond 8810	1
6	MATFIN Server	HP Proliant	1
7	APAR Server	HP Proliant ML 350 Gen 9	1
8	MyNEEPCO Server	IBM 7975	1
9	Replica server (Attendance, Commercial Billing, Inventory, etc.)	HP Proliant	1
10	Primavera Server	IBM 7976	1
11	SAN Storage	IBM DS5100	1
12	Router (HCL Comnet)	Cisco 2600 Series	1
Grand Total			18

2. List of Applications for vulnerability assessment

Sl. No.	Application name	Description
1	Matfin	Host centric database Application for Materials and Financial Management System (accessed through client terminal emulator)
2	MyNEEPCO Portal	Web-based portal for NEEPCO Employees
3	Commercial Billing Software	Web-based monthly billing system for beneficiary states
4	Fixed Asset Web module	Web Application for fixed asset inventory management
5	APAR Software	Online web application for annual performance appraisal reporting for NEEPCO Employees

PRICE SCHEDULE A

Sl. No.	Description of Items	Unit	Quantity	Basic charge in INR (Exclusive of Taxes & Duties)	Amount of Taxes and Duties (From Price Schedule B)	Total quoted price in INR inclusive of all applicable taxes and duties	Total quoted Price in INR inclusive of all applicable taxes and duties in Words
A	B	C	D	E	F	$G=(E + F) \times D$	H
1	Vulnerability Assessment of IT hosts/ devices as listed at sl. 1 Annexure 1 and as per scope defined in Bid Document	Lot	1	82302.00	14814.36	97116.36	Rupees Ninety Seven thousand One hundred Sixteen and paise Thirty Six
2	Security Audit of IT applications and Web Applications as listed at sl. 2 Annexure 1 and as per scope defined in Bid document	Lot	1	117015.00	21062.70	138077.70	Rupees One lakh Thirty Eight thousand Seventy Seven and paise Seventy
3	Security Assessment of IT Operations and Processes for the scope of work as per technical specifications and scope defined in Bid document	Lot	1	110005.00	19800.90	129805.90	Rupees One lakh Twenty Nine thousand Eight hundred Five and paise Ninety
TOTAL				309322.00	55678.00	365000.00	Rupees Three lakh Sixty Five thousand



PRICE SCHEDULE – B (FOR TAXES and DUTIES)

Sl. No.	Description of Items	Description OF Taxes / Duties / Levies with HSN/ SAC Codes	Percentage Rate of Taxes / Duties / Levies applicable	<u>Amount</u> in INR on which Taxes / Duties/ Levies applicable	<u>Amount</u> in INR of Taxes / Duties/ Levies payable
A		B	C	D	E
1	Vulnerability Assessment of IT hosts/ devices as listed at sl. 1 Annexure 1	GST	18%	82302.00	14814.36
2.	Security Audit of IT applications and Web Applications as listed at sl. 2 Annexure 1	GST	18%	117015.00	21062.70
3.	Security Assessment of IT Operations and Processes for the scope of work as per technical specifications.	GST	18%	110005.00	19800.90
Total <u>Amount</u> of TAXES / DUTIES/ LEVIES payable					55677.96

