CHAPTER-14
ANNEXURE-37
(Clause 14.2)

e-Procurement and e-Reverse Auction

1. **Specific requirements of e-Procurement System**

The service provider in consultation with the Purchaser shall establish the following process:

- The service Provider / Purchaser should not be able to reduce the essential security and transparency aspects of the system on the pretext of re-engineering and customization.
- Bids before transmission from the bidder's computer should be protected with SSL Encryption.
- e-Procurement System must have templates to offer flexibility in bidding methodology as prevailing and followed currently in the manner of processing. Further, the system should have templates to adopt bidding methodology as may be prescribed by the purchaser.
- e-Procurement System should deploy PKI based technologies for authenticating the bids and opening electronic tender box. Secure methodology for decrypting bids should be deployed corresponding to the encryption methodology deployed (viz. symmetric, or PKI-based asymmetric). The entire IT hardware infrastructure of e-Procurement System which includes application software, hardware, and system software be hardened as relevant. The system must deploy anti-spyware and anti-spam with a provision to update regularly. The updation of these software on the e-Procurement System be done using the offline updation mode. The e-Procurement System must have software tools to protect the operating system from injection of spyware. The entire infrastructure should be protected and secured at the perimeter level by installing firewalls and Intrusion Prevention System. The system should be configured properly so as to detect any kind of intrusion into IT system.
- e-Procurement System can be further secured by installing suitable security incident and event management mechanisms SIEM (Security Incident Event Management).
- The PKI Key Management System for authenticating the bids or other purposes must specify the holder of private key and public key. The procedure in this case may be prescribed.

2. **Requirements of Conformity**

i. e-Procurement systems must address:

- E-procurement application should have provisions of ensuring validation of PKI signature through Certificate revocation list (CRL) and validity of certificate.
- Shall have mechanism for time synchronization by using time synchronization service (TSS) at hosting level, or synchronization with master-server at the data center where the e-procurement system is hosted.
- Time Stamping facility should be there in the e-procurement application for time-stamping of all important events like – creation of tender notice, approval of tender notice/ tender documents, submission of bids and supplementary bids(like modification, substitution, alternatives), etc. Time Stamping is critical for establishing date and time of document submission and its acknowledgement. Time Stamping feature should be built within the application and synchronization of e-tendering/ e-procurement server should be done with master server at the data-center where the e-procurement system is hosted. Alternatively, the e-procurement service provider can take Time Stamping services being provided by licensed Certifying Agencies (CAs).
- The system must be in line with GFR rules and Information Technology Act (including amendments) and other laws of the land as applicable.

ii. Other Requirements for Quality and Security Evaluation:

- The e-procurement application should have facility for generating audit-logs, which should be accessible (in downloadable form) to a specially designated officer of the Purchase organization or e-procurement service provider shall submit all the logs of transaction created by the e-procurement solution including forensic image on quarterly basis or as prescribed by the user organization regularly and as and when demanded by the purchasers. The logs will be duly signed by the administrator of the service provider by his electronic signature.
- The audit for certification of the entire e-procurement solution shall be undertaken after its deployment and prior to its usage.
- The e-procurement solution including the computer server shall be installed in India. No data as captured/stored in the e-procurement solution will be taken out of India. However, bidder outside India should be able to quote and download permitted data/information.
- The e-procurement solution shall need to be tested and audited again after it has been significantly modified (addition/ deletion of functions/ modules) or customized for a new organization whether stand alone or shared mode.
- The traffic emanating to and from e-Procurement systems will be scanned if required by the authorized body. The traffic (net flow)

emanating to and from e-Procurement System may be provided to CERT-IN[18].

3. **Guidance and recommended practices- e-Procurement System**

a). The underlying principle of e-tendering and manual tendering process should be same in respect of guidelines of GFR, Legal and transparency related requirements.

b). Depending upon the requirements of a tender, any one of the multiple bidding methodologies as outlined below shall be provisioned in the application:

- Single-stage, single- envelope
- Single-stage, two- envelope
- Two stage (with facility for 'technical conformance', and if required, 'revised tender documents')
- Two-stage, two- envelope and requirement of Pre-qualification stage when required submission of one or more Alternative bids as applicable.

c). Each bid part (e.g. technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file. There should be provision of appropriate file size (at least 10 MB) in the application with data encryption.

d). After having submitted the 'original' bid for each bid-part and before the due date and time for submission of bids, a bidder has a right to submit:

- 'Substitution' bid; or
- 'Withdrawal' bid for all its bid-submissions.

e). The e-tendering system must effectively cater to all these possibilities without compromising security and transparency in any manner at any stage, for any bid part (such as Pre-qualification, Technical, and Financial).

f). The controls should be placed to guard against the possibility of injecting spyware for making clandestine copies of a submitted bid and then sending this clandestine copy to a secret destination.

g). Even if a clandestine copy is made and stolen as above, the bid encryption methodology should be such that it should not be possible to decrypt the bids in connivance with any officer of the Buyer organization or the Service Provider organization.

h). The e-procurement system should have audit trail facilities. These audit trails are complex but dependable. The audit trails reports provide useful information about the instructions which take place in the

[18]Indian Computer Emergency Response Team

system both at operating system and application software. This information is necessary to analyze nature of intrusion, vulnerabilities exploited and to track the perpetrators. It also helps in taking steps in preventing future intrusion.

i). Secure submission of bid from bidder's computer to the server should be done after the bid file is encrypted (with symmetric or asymmetric encryption) at the bidder's computer and further submitted to the e-procurement server through SSL encryption. Only the encrypted file submitted by the bidder should be stored and should be decrypted at the Tender Opening Event (TOE).

j). Under the IT Act, 2000 any holder of a Digital Signature, whose Digital Signature Certificate (DSC) has been issued by a licensed Certifying Authority (CA), is responsible for protecting the corresponding private key. Unless the certificate validity has expired or the certificate has been revoked by the issuing CA, any digital signature will be legally valid and will be attributed to the person listed in the DSC. Similar mechanism measures should be evolved for encryption key pair as well.

k). Handing over of private (decryption) key by one officer to another officer both in case of digital signature as well as in case of encryption should not be allowed.

l). In case of digital signature, private key should be one of the two factor authentication method which must be implemented. The other could be Personal Identification Number (PIN) or biometric etc., so that nobody else can use the private key for signing the document.

m). Tender documents posted on an e-tendering/ e-procurement website should be digitally signed by an officer of the tendering organization and for the assurance of the bidder who is viewing or downloading the tender documents, the e-procurement system should have functionality to verify the digital signature to ensure the authenticity and integrity of the tender documents.

n). It should not be possible to open the 'e-tender boxes' till the specified time has occurred or elapsed, and till all the authorized Tender-Opening Officers have formally instructed the system to do so with PKI-based Digital Signatures.

o). Till the Public Tender Opening Event, security related features should be such that the contents of the bids which are being stored cannot be 'accessed and decrypted' by even the authorized officers of the Purchaser/ Buyer or the Administrators of the Service Provider.

p). e-procurement System should have functionality for 'Not Accepting Late Bids' i.e. bids received after the specified date and time for receipt of bids.

q). The GFR requires that tenders be opened in public in the presence of the authorized representatives of the bidders. The Finance Ministry Manual on procurement procedures outlines in detail the requirements

of a transparently conducted Public Tender Opening Event. A comprehensive and transparent Public Tender Opening Event is the 'backbone of transparency and fairness' of the Public Procurement process, manual or electronic. This has an impact on technical as well as procedural aspects.

r). It must be ensured that e-tendering/e-procurement has comprehensive functionality for a transparent Public Online Tender Opening Event (TOE). Well established practices of manual tender opening should have corresponding electronic equivalents for transparent e-tendering/ e-procurement. Some relevant processes of a fair and transparent online public TOE should include:

i. Opening of the bids in the online presence of the bidders who choose to be present. Merely opening bids 'online', and then separately making them available for display to the bidders subsequently, and/ or from a different location/ screen (i.e. user interface) without the online presence of bidders, does not fulfill the requirements of a proper and transparent online Public TOE.
ii. Security Checks to assure bidders of non-tampering of their bids during the online TOE itself.
iii. One-by-one opening of the sealed bids.
iv. Online verification of the digital signatures of bidders affixed to their respective bids.
v. Reading out, i.e. allowing bidders to download the electronic version of the salient points of each opened bid (opened in the online presence of the bidders).
vi. Digital counter-signing (by all the tender opening officers) of each opened bid.
vii. Preparation of the 'Minutes of the Tender Opening Event', its signing by the concerned officers and uploading.

While bidders should be welcome to be present online during the TOE, it should not be mandatory for them to do so. There should be proper online attendance record of the bidders, who choose to be present.

However, the above stipulations are not followed in case of e-Reverse Auction as per CIL's approved guidelines.

s). The Administrators of the e-tendering application/portal should not have any access to the passwords of the various users. Neither the software should allow the Administrator to generate password for the users. E-Procurement System further should not have "forgot password" feature which provides administrator-generated or system-generated temporary password. Once the password is forgotten, a new password may be allotted following a set of processes needed for allotment of password. The forget password request shall be digitally signed.

t). Generally any system is designed in such a manner that it gets locked/denied permission after repeated login attempts based on wrong passwords and/or user IDs. Such a scenario, if it exists, in e-

procurement system may be exploited by the competitors to prevent the genuine bidders. To avoid such a situation the e-procurement system should not have features for locking the system on account of repetitive login attempts based on wrong passwords and/or user IDs and digital signatures. Login to the e-procurement system should be based on digital signatures.

u). The e-tendering system should have facility for displaying 'Award of Contracts'. Furthermore, this information should be digitally signed by the concerned user of the Buyer organization with facility for verification by the viewer.

v). In case of 'Buy Back Offers', the e-procurement System should have functionality where 'Buy Back Price' should also be captured in the Financial-Bid and provision should be there for 'Net Procurement Price' after taking into account the 'Buy Back Price'.

4. **Service Provider**

A Service Provider will be engaged by CIL for CIL and its subsidiary companies. The e-procurement system and processes used by the Service Provider shall have to be compliant to all the applicable Laws of India, GFR, as also to the directives / instructions issued by Ministry of Electronics and Information Technology (MeitY), Ministry of Finance and Ministry of Coal of GOI.

5. **Scope**

The e-procurement system will cover the following:

- Various steps involved like hosting of NIT, downloading and submission of bids, online opening of bids, on-line TPS based evaluation of bids, opening of price bids and reverse auction on a dedicated e-procurement portal of the company.
- Archiving of information and generation of reports for MIS/ Decision Support System of CIL/ Subsidiary Companies.
- A helpdesk for online and offline support to different stakeholders.

6. **The Organizational Setup**

An e-Procurement Cell shall be at CIL(HQ) and each Subsidiary Company HQ with following responsibilities:

a). To co-ordinate and correspond with Service Provider, Bidders, User Departments and other concerned authorities such as Banks, Auditors etc. for the effective and efficient implementation of e-Procurement.

b). Arrangement of Training to Bidders and Departmental Officers for working on e-Procurement mode.

c). To coordinate for the infrastructure development for the proper implementation of the e-Procurement system.

d). To create a helpdesk for online and offline support to different stakeholders of the system.

e). To arrange and update the Digital Signature Certificate for departmental users.

f). To finalize the different documents, formats, etc. for the e-Procurement system.

g). To Administer the e-Procurement Application and Online User Management