Managing Hybrid Outsourcing /42 Touch Me Not /36 Follow Dataquest on twitter | ₹50

www.dqindia.com

DATAQUEST

Vol XXIX No 08 | April 30, 2011 The Business of Infotech

A CYBER MEDIA publication

How India Did it

Social networking emerges as the real battle-winner in Anna Hazare's movement

92 pages including cover

Special subscription offer on Page 76

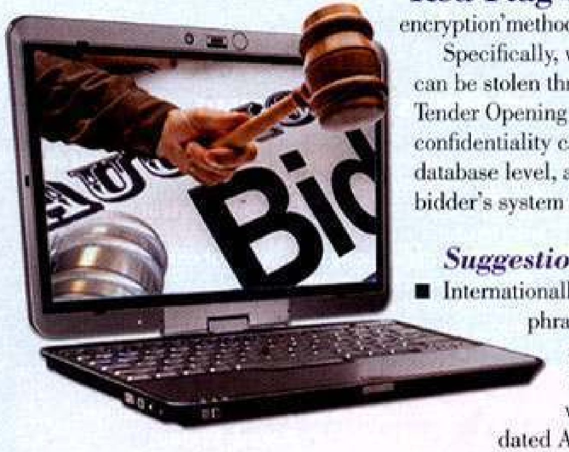
E-procurement: The Red Flags

Procurement could well be the potential Waterloo in the fight against corruption. A look at the common malpractices and how to avoid them

The reasons for the increasing tendency to switch to e-procurement in recent times are certainly speed and efficiency. But in the government space—especially in a democracy—no advantages can substitute the need for national security and transparency. In fact, if anything, e-procurement should be better than manual tendering in these aspects of security and transparency.

While changing over to e-tendering/ e-procurement, it must be ensured that under the pretext of reengineering, the e-procurement software does not in any way compromise on legal, security and transparency related aspects of public procurement. Well established practices of manual tendering (especially those relating to security and transparency) should have corresponding electronic equivalents in e-tendering/ e-procurement.

There could be many areas of compromise/attempted compromise of security and transparency in an e-procurement process. Here are the most common ways of manipulating the e-procurement process. Let us call them the red flags.



Red Flag #1: In most e-procurement systems, the 'Bid-sealing/Bid-encryption'methodology is poor/ flawed.

Specifically, where PKI is used for bid-encryption, clandestine copies of bids can be stolen through spyware and secretly decrypted before the Online Public Tender Opening Event, resulting in compromise of confidentiality. Similarly, confidentiality can be compromised where the 'main bid-encryption' is done at database level, and only SSL encryption is done during the transit phase from bidder's system to the e-procurement portal.

Suggestions:

- Internationally acceptable forms of bid encryption include symmetric pass-phrase and asymmetric key (PKI). 'RFPs for e-procurement' should allow both forms of bid encryption. However if asymmetric key is used for bid encryption, the RFPs should specify that security vulnerabilities as described in CVC circular No.18/04/2010 dated April 26, 2010, especially security checkpoint at S No 14 of this

> **The focus of the current IT Act is on use of 'digital signatures' for authentication, non-repudiation, and data-integrity of electronic records**

circular must be addressed by the e-procurement software provider with proper explanation.

- There is a 'misconception' that the IT Act 2000 recommends the use of PKI for data encryption (ie, bid encryption in the context of e-procurement). This is not correct. The IT Act does not prescribe any method of data encryption.

The focus of the current IT Act is on use of 'digital signatures' for authentication, non-repudiation, and data-integrity of electronic records. Guidelines under s-84A of the amended IT Act 2000 in respect of 'Data Encryption (ie, bid encryption in the context of e-procurement) are pending.

Data Security Council of India (DSCI) in its 'Recommendations for Encryption Policy' u/s 84A of the IT (Amendment) Act, 2008, for 'Data Encryption' (ie, bid encryption in the context of e-procurement), has suggested the use of 'symmetric encryption', and cautioned against the use of 'asymmetric encryption' for 'data encryption'.

Sections II and III of the 'e-Procurement Integrity Matrix' (published on TII site—http://transparencyindia.org also highlight security concerns relating to use of Public Keys of the TOE officer for bid encryption, and/ or if main encryption of the bid is done at the database level.

Till the central government prescribes the modes or methods for encryption u/s 84A, guidelines may be issued in line with recommendations of DSCI, or at least the above mentioned misconception should be clarified.

Red Flag #2: In most e-procurement systems, instead of 'Online Public Tender Opening Event', there is only a rudimentary 'Online Tender Opening'. Merely opening bids 'online', and then separately making them available for display to the bidders subsequently, and/or from a different location/screen (ie, user interface) without the simultaneous online presence of bidders, does not fulfill the requirements of a proper and transparent online public TOE. The transparency related significance of opening bids in 'public', and carrying out various activities such as 'countersigning' of each opened bid by the TOE officers in the simultaneous presence of the bidders has been given done away with. E-procurement systems where online TOE is conducted in this non-transparent fashion, without the simultaneous online presence of the bidders, gives rise to the possibility of bid-data tampering.

Suggestions:

A comprehensive and transparent Public Tender Opening Event is the 'backbone of transparency and fairness' of the public procurement process, manual or electronic. It must be ensured that e-tendering/ e-procurement has comprehensive functionality for a transparent Public Online Tender Opening Event (Public OTOE).

Some relevant processes of a fair and transparent online public TOE should include:

- Opening of the bids in the simultaneous online presence of the bidders with proper online attendance record. Merely opening bids online, and then subsequently displaying some results to the bidders does not fulfill the requirements of a transparent Online Public Tender Opening Event
- Security Checks to assure bidders of non-tampering of their bids, et al during the online TOE itself
- One-by-one opening of the sealed bids in the simultaneous online presence of the bidders
- Reading out, ie, allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of the bidders)
- There should be a procedure for seeking clarifications by the TOE officers during online Public TOE from a bidder in the online presence of other bidders, and recording such clarifications
- Digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders
- Preparation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders

Red Flag #3: Most e-procurement systems do not have the functionality to accept 'encrypted (ie, sealed) detailed bids. Some systems 'do not encrypt the technical bid at all', ie, neither the electronic template of the technical bid, nor the detailed technical bid. In such systems, typically 'only summarized financial data in electronic templates' is encrypted. This is against the established practices of ensuring confidentiality of technical bids.

Suggestions:

As in the manual tendering process, all bid envelopes, viz, technical, financial, and prequalification, should be sealed, ie, suitably encrypted by the bidders in the e-tendering/e-procurement system. In e-procurement systems, a bid envelope may consist of an electronic form, and an accompanying detailed bid for some envelopes. All bid parts must be encrypted and digitally signed. If required, printed brochures, manuals, physical samples etc can be submitted offline.

Red Flag #4: Many e-procurement systems do not have the functionality for digital signing of important electronic records which are part of the e-procurement application. As a result, such e-procurement systems are not in full compliance of the IT Act 2000, and certain guidelines of the CVC.

Suggestions:

Use of digital signatures must be as per the letter and spirit of the IT Act 2000 and its subsequent amendments for the purpose of authentication, non-repudiation, and integrity of all important electronic records. Such electronic records should include tender notices and corrigenda, tender documents and addenda, online clarification of tender documents sought by the bidder, signing of bids (including modification and substitution bids) by the bidder, online counter-signing of all opened bids by the tender-opening officers in the online presence of bidders, and online minutes of the tender opening event. Facility should be provided within the e-tendering/e-procurement system to 'verify' digital signatures which have been affixed to the electronic records.

Red Flag #5: In most e-procurement systems, functionality of the e-tendering system is limited (eg, all types of bidding methodologies are not supported). In some cases only 'single-stage-single-envelope' bidding is supported. Similarly many systems do not support the submission of 'supplementary bids viz, modification, substitution, and withdrawal' after final submission, but before elapse of deadline for submission. This is against the established practices of manual tendering.

AS IN THE MANUAL TENDERING PROCESS, ALL BID ENVELOPES, VIZ, TECHNICAL, FINANCIAL, AND PREQUALIFICATION, SHOULD BE SEALED, IE, SUITABLY ENCRYPTED BY THE BIDDERS IN THE E-TENDERING/E-PROCUREMENT SYSTEM

Suggestions:

The e-tendering system should support all established bidding methodologies, viz, single-stage single-envelope, single-stage two-envelope, two-stage, two-stage two-envelope, these bidding methodologies preceded by pre-qualification. Where required by the purchaser, the e-tendering/e-procurement system should support submission of 'alternative' bids, as well as, submission of 'modification', 'substitution', and 'withdrawal' bids by the bidders.

In fact, CVC Circular 01/02/11 dated Feb 11, 2011 suggests use of 'two-stage' bidding methodology with provision for 'Revised Tender Specifications' under certain circumstances. In this case, the financial bid is not submitted in stage-1.

Red Flag #6: 'Entry Barriers' are being created in many RFPs for e-procurement, on the entry of new players on the basis of 'unjustified eligibility criteria', and by insisting on 'irrelevant experience'.

Caution: It must not be forgotten that e-procurement is an emerging technology, and if entry barriers are created, apart from discouraging competition, the government will not have the benefit of better and more reliable e-procurement systems. Furthermore, experience of tenders conducted using 'rudimentary e-procurement software' would not only be irrelevant but misleading.

Suggestions:

- E-tendering/e-procurement is a new methodology/technology for public procurement the world over. It is also well known that initial projects in e-tendering/e-procurement in the country had very rudimentary security features and limited functionality. It is important to have new players in this area with high levels of security and comprehensive functionality in their e-tendering/e-procurement software. To achieve this objective, it is important that such new e-procurement software/ service providers are not kept out of competitive tendering by imposing eligibility criteria which require prior experience of hundreds/thousands of tenders.
- To encourage competition, and at the same time not waste time in experimentation, eligibility criteria should essentially ask for a 'ready-to-use' e-tendering/e-procurement software (without any need for customization for the main tendering processes), which is tested and certified, and can be delivered immediately. The functionality of the

software can be thoroughly tested before signing the contract, through demo/pilot tenders. The main focus should be on the functionality of the software in terms of security, transparency, and comprehensiveness. Where absolutely necessary, experience of a few actual tenders (say 25, or even less), of the types relevant to the organization and meeting the security-checks criteria outlined in the CVC circular No. 18/04/2010 dated April 26, 2010, may be sought as part of the eligibility criteria.

The main tendering processes of government organizations are all within a standard framework, so there should be no need for customization for each project, except possibly for 'integration with other applications'.

Red Flag #7: Many e-procurement systems are such that it results in abdication of powers of the concerned officers of the government purchase department. Furthermore, in some situations it results in handing over the private keys (PKI) of the concerned officers to others, which is a violation of s-42(1) of the IT Act.

Suggestions:

- Changing over to e-procurement does not imply that the powers and duties of the officers (including those under the Official Secrets Act) for the core tendering processes can be passed on to 'private third-party service providers', or to a few technical personnel within the purchaser organization. Each officer, who currently enjoys powers and has responsibilities relating to the procurement activities, should be able to exercise the same under the e-procurement system. The e-procurement system should support such functionality by facilitating a comprehensive hierarchy of officers, with specific role authorization facility.
- Rules should prohibit the engagement of 'private third parties' for outsourcing the core tendering processes, unless proper checks are put in place. Most importantly, third parties should only be 'e-procurement platform providers', and 'not e-procurement service providers'.
- Sensitive organizations like Defence, should even manage the e-procurement platforms/portals themselves, and only source/ license the software from e-procurement software developers.

Red Flag #8: There is lack of clarity about where e-reverse auction is to be used. It is obvious that the government does intend to replace sealed-bid tendering with e-reverse auction. Also there are guidelines about 'not negotiating' after the financial bids are opened, except possibly with L1 (which is contrary to the concept of reverse auction). At the same time, reverse-auction could be useful in some situations, eg, commodity purchases. In such a scenario it is important to clarify where reverse auction can be resorted to.

THE MAIN TENDERING PROCESSES OF GOVERNMENT ORGANIZATIONS ARE ALL WITHIN A STANDARD FRAMEWORK, SO THERE SHOULD BE NO NEED FOR CUSTOMIZATION FOR EACH PROJECT, EXCEPT POSSIBLY FOR 'INTEGRATION WITH OTHER APPLICATIONS

Suggestions:

The following may be clarified:

- Reverse auction is not a substitute for the sealed-bid tendering process.
- It can be resorted to as per guidelines issued by the Central Vigilance Commission, the Finance Ministry and other regulatory bodies from time to time. Such situations may be explicitly outlined.
- Where allowed, it could be a follow-up activity to preceding sealed-bid steps of etendering/e-procurement. In such a case, the reverse auction should be available in an integrated and seamless manner to the preceding sealed-bid steps of e-tendering/e-procurement.
- Use of digital signatures must be as per the IT Act 2000 and its subsequent amendments for the purpose of authentication, non-repudiation, and integrity of all important electronic records, as in case of e-tendering/ e-procurement. Specifically, the final offers of the bidders must be digitally signed by the concerned bidders, and digitally counter-signed by the concerned officers conducting the reverse auction.
- Minimum Entry Barriers and related Eligibility Criteria: Similar to the rules for e-tendering/e-procurement. (Similar guidelines may also be issued for e-forward auction with minimum entry barriers.)

Also, most of the certificates that vendors often boast of are minimum qualifications and should be treated as necessary but not sufficient requirements. But many a times, they are taken as certificates of excellence. Security tests like Cert-In, STQC, OWASP are useful but general in nature, and do not have anything specific to address the intricacies of e-procurement. 'e-Procurement Certification' related Govt guidelines (as mentioned in CVC Circular No. 23/06/010 dtd June 23, 2010) are still awaited. ■

JITENDRA KOHLI

The author is a member of Transparency International India. The article is roughly based on his presentation made at the National Workshop on Integrity Pact held recently
maildqindia@cybermedia.co.in