RED FLAGS IN E-PROCUREMENT/ E-TENDERING FOR PUBLIC PROCUREMENT AND SOME REMEDIAL MEASURES

Jitendra Kohli*

ABSTRACT. Essentially, e-Procurement/ e-Tendering is conducting on the internet the equivalent of the manual tendering process, with the ostensible objective of enhancing Transparency and Efficiency of Public Procurement. While this naturally involves some re-engineering, it is important to ensure that under the pretext of re-engineering and technology, there should be no compromise on the security/ confidentiality, transparency and legal aspects of the well-established public-procurement process. The focus of the paper/ presentation will be on some such critical issues, or red flags, with suggestions for remedial measures.

** Jitendra Kohli, B.Tech. (Electrical Engg) IIT Delhi (India), founder and Managing Director of ElectronicTender, has been researching in the area of e-procurement/ e-tendering with focus on public procurement for over 12-years now. Based on his pioneering work, his company, ElectronicTender has developed an innovative e-procurement/ e-tendering software product with comprehensive security and transparency related features required in government tendering. This product can be licensed for being readily deployed in any country for setting up e-procurement/ e-tendering portals with 'Nil' gestation period. His work, 'e-Procurement Integrity Matrix' has been adopted and published by Transparency International India (Reference-1). The Government of India's guidelines for e-procurement (Reference-2) have taken inspiration from his writings on the security and transparency related aspects of e-procurement. His services were recently commissioned by the Asian Development Bank for technical peer-review of the update of MDB's 'e-Procurement Toolkit'.*

INTRODUCTION

Some Distinctive Aspects of Government Tendering/ Public-Procurement Process: Public procurement constitutes 10% to 20% of the GDP in various countries. In addition to buying at the most economical price, the distinctive and 'stated-principles' of public procurement have been to ensure -- *Transparency*, *Fairness* and *Accountability* in the procurement process. Procedures for public-procurement have been developed to implement these stated-principles. Starting with advertising a bidding opportunity in a national-level newspaper for wider publicity, elaborate procedures exist in most countries for activities relating to the tendering process, which inter alia includes processes such as – 'Signing of each page of the bid by the bidder' to ensure authenticity, 'Bid-Sealing' to ensure confidentiality and independence of each bid, a fair and transparent 'Public Tender Opening Event' with its detailed procedures to ensure fair-play, et al.

E-Procurement, an emerging Methodology for Public Procurement: 'e-Procurement' or 'e-Tendering' is the emerging method for conducting 'Public Procurement' using the internet. As the name suggests, an e-procurement system/ portal will be accessed through the internet by authorized users of a Buyer organization, as well as, authorized users of different Supplier/ Bidder organizations for conducting various activities relating to the tendering process, ie bid invitation and response process, from the comfort of their respective offices. From Buyer and Supplier perspectives, an end-to-end e-procurement system is expected to offer broad functionality as outlined in Annexure-I of this paper. The depth and quality of implementation of each module may vary in each system, till standards emerge and are followed.

Overall, in terms of adoption and implementation, e-procurement is still in a nascent phase globally. While some countries like India are making e-procurement mandatory for Government procurement above a certain threshold value, many countries, including advanced countries in North America and EU, currently have limited e-procurement implementations for public procurement with rudimentary security features. However, the stated intent in many countries is to encourage e-procurement, as the potential benefits of e-procurement are compelling.

'Need for Re-engineering', and 'Need for Avoiding the Possibility of Cutting Corners on the Pretext of Re-engineering': With evolving technology, procedures inevitably undergo change. As stated earlier, public procurement involves mammoth public expenditure in every country, and as an unfortunate consequence of this, scams and controversies have been associated with this sensitive area. Therefore, any re-engineering of the public procurement methodology while shifting from the manual tendering methodology to internet-based methodology (ie e-procurement), should be done with adequate due-diligence of the new methodology, and by taking adequate cognizance of loopholes of the new methodology. Specifically, in the process of re-engineering, the stated-principles of public-procurement should not be relegated or cast aside. However, the actual implementations of e-procurement in many countries are found wanting in this respect.

Benefits of e-Procurement: and some Associated Conditionalities: Undoubtedly, if e-procurement is done with proper security and functionality, it holds enormous potential for enhancing efficiency and transparency in public-procurement internationally, apart from the obvious benefits such as savings in time and cost, wider reach, et al. However, dearth of awareness about the intricacies of e-procurement/ e-tendering, especially aspects relating to 'Security' and 'Transparency', is resulting in proliferation of e-procurement portals in many countries which have numerous lacunae and pitfalls. In fact, many of the projected benefits of e-procurement are contingent upon the measures adopted in the e-procurement system (especially the e-procurement application software) to ensure security and transparency. A list of 'Salient Benefits of e-Procurement' is enclosed as Annexure-II. Needless to state, *unless these lacunae and pitfalls are properly addressed with appropriate security and transparency related measures, e-procurement could actually be worse than the traditional manual procurement/ tendering process* in respect of preventing manipulation and corruption.

The issues and remedial measures relating to secure e-procurement highlighted in this paper are based on the author's direct involvement for over twelve years in the process of innovation, original research and development of cutting-edge 'e-procurement application software'. Another noteworthy aspect is that while there is technical literature available, such as 'Reference Document-3', on the elements and tools (such as PKI-based digital signatures, symmetric and asymmetric keys/ tools for data encryption) which go into building an e-procurement application, there is very little detailed literature available on the 'technical intricacies' of a 'secure e-procurement application'. 'Reference Documents 1 and 2' are perhaps the most comprehensive documents addressing this need, which are available in public domain. Both these reference documents are inspired from the research and writings of the author. The present paper is another such document.

During the forthcoming IPPC5 conference, the author intends to make a presentation on the same subject with emphasis on a few select 'Critical Security Issues and Loopholes relating to e-Procurement Web-Application', which will elucidate some of the issues highlighted in this paper, as well as, set the backdrop for the paper.

OBJECTIVE

The objective of this paper is to highlight in a concise manner a few 'Security' and 'Transparency' related lacunae or 'Red Flags' in e-procurement, so that Government entities which implement e-procurement do so in a proper manner.

Note-1: While some references of legal acts are in respect of India, the main points made under the various 'Red flags' would be applicable for all countries.

Note-2: While highlighting the lacunae in the existing e-procurement systems, the author has deliberately avoided giving references of specific projects in different countries, although this information may be available with the author. It is left to the concerned authorities in each country to conduct a technical review of their respective e-procurement implementations, and take corrective action.

THE RED FLAGS

Overall Guiding Principle for Addressing the Red Flags: In terms of 'security and transparency', e-procurement should be better than the 'manual tendering' process, or at least as good. It certainly cannot be accepted if it is worse in this respect. Well established practices of manual bidding (or tendering), especially those relating to security and transparency, should have corresponding functional equivalents in e-tendering/ e-procurement application.

(**Red Flag No.1**): **In many current e-procurement systems, the 'Bid-sealing/ Bid-encryption' methodology is non-existent, or poor/ flawed.**

<u>Background</u>: In the manual process of bidding or tendering, bids are sealed in paper-envelopes to ensure 'confidentiality' of the bid before the Public Tender Opening Event (Public-TOE) from not only competitors, but also officers of the procuring entity. Sealing a bid in a paper envelope makes the bid data 'unreadable'. There has to be a functional equivalent of this in the electronic system also.

A re-engineered functional equivalent of a 'sealed envelope' can be an 'encrypted bid'. The process of encrypting the bid data achieves the objective of making the bid data 'unreadable', until it is decrypted during the Public-TOE.

However, if no such functional equivalent is provided in the re-engineered electronic system, or a vulnerable form of bid encryption is provided, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

<u>On-the-Ground Situation in Flawed e-Procurement Implementations</u>: The flawed e-procurement implementations fall into two broad categories;

Category-1: In such systems, the online bids which are submitted by the bidders are not encrypted at all. This would tantamount to bids being submitted without sealed envelopes. Administrators of the e-procurement portal and those having access to the database can peep into the contents of bids to help some preferred bidder(s), and thus compromise the 'confidentiality' aspect of the process. Such e-procurement systems are too unsecured and basic to be used for public-procurement.

Category-2: Bids are encrypted, but the bid encryption methodology is inappropriate for the requirement of secure public procurement. Now, essentially, there are two broad methods of data-encryption (ie bid-encryption in the context of e-procurement), viz – 'symmetric' and 'asymmetric'. Specifically, where asymmetric key (eg public-key of the bid-opening officer of the procuring entity) is used for bid-encryption, clandestinely made copies of bids can be stolen through spyware and secretly decrypted before the Online Public-TOE resulting in compromise of confidentiality. Similarly, bid-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. In such systems, there are many other allied deficiencies relating to functionality and transparency. If system-generated symmetric-key is used for bid-encryption, it also has vulnerabilities as a copy of the key may be accessed by the system administrator for clandestine decryption prior to the Online Public-TOE. For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* (e-Procurement Integrity Matrix, especially sections II, III and partially IV); *Reference-2* (e-Procurement Guidelines, Annexure-I, especially sections 2, 3, and partially 4); *Reference-3* (Applied Cryptography, pp 33).

To justify the application of PKI for bid encryption in spite of the associated security vulnerabilities as briefly explained above, a 'misconception' is often propagated by vested interests that the Information Technology Act 2000 (*Reference-4*), ie IT Act, 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. Digitally signing an electronic document or record (or data) does not encrypt the data, ie it does not 'secrete' the data. The digital signature (which is created by first producing a one-way hash of the data being signed, and then encrypting the hash with the private-key of the signer) is distinct from the original record (or data) of which the signature has been created. The signature thus created can be kept separate from the original data. In this case, the original data (or record) remains as readable after the signature, as it was before the signature.

It may please be noted that highlighting the vulnerabilities of PKI based bid-encryption in the context of public procurement should not be construed as a sweeping criticism of the use of PKI for any form of data encryption. The criticism is only in respect of its use for bid-encryption in the specific context of public procurement. The merits and demerits of any tool or methodology have to be weighed with reference to the relevant context or situation.

Note-3: Each country is enacting its own electronic signature act. The Indian IT Act 2000 is also inspired from the corresponding UN Model law. The General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 adopted the Model Law on Electronic Commerce, adopted by the United Nations Commission on International Trade Law.

Furthermore, reputed international textbooks on cryptography have also clearly highlighted the limitations of asymmetric key based data encryption, especially in respect of its 'slowness' and 'vulnerability'. For a more detailed explanation of the issues, the reader may refer to -- section 2.5 titled 'Communications using Public-Key Cryptography' of 'Applied Cryptography' by Bruce Schneier (*Reference-4, pp 33*)

Brief Remedial Suggestions:

As stated above, internationally acceptable forms of bid encryption include – *symmetric-key*, and *asymmetric-key* (also referred to as PKI in some countries). Bid-encryption using 'bidder-created symmetric key/ passphrase' has distinct advantages (including being free of the vulnerabilities mentioned above), and has been used for the purpose of bid-encryption in the software of ElectronicTender developed under the guidance of the author. Where 'Requests for Proposals (RFPs)' for e-procurement systems allow both forms of bid encryption, the RFPs should specify that security vulnerabilities as described in sections II and III of the 'e-Procurement Integrity Matrix' (*Reference-1*) and sections 2 and 3 of Annexure-I of e-Procurement Guidelines (*Reference-2*) must be satisfactorily addressed by the e-procurement application software provider with proper explanation. These explanations should be thoroughly vetted and tested by the Government department using the system as a procuring entity.

(**Red Flag No.2**): **In most e-procurement systems, instead of 'Online Public Tender Opening Event' (Online Public-TOE), or Bid Opening Event, there is only a rudimentary 'Online Bid Opening'.**

Background: In the manual process of bidding or tendering, the sealed bids are opened in public, ie in the presence of the bidders who have submitted bids for a particular tender. Salient points of each bid are read out aloud, and each page of each opened bid is counter-signed by one or more tender-opening officers of the procuring entity. This is to ensure transparency and fair play. As per established principles of public-procurement, it is intended that in this event, each bidder should know what the other bidders have quoted, so that no unfair and clandestine changes are made later due to any connivance between a bidder and the procuring entity officers.

A re-engineered functional equivalent of the manual Public-TOE would be an 'Online Public TOE', in which the bids are opened online by the authorized tender opening officers of the procuring entity in the simultaneous online presence of bidders, along with other important procedures such as digitally counter-signing of the bids online by the TOE-officers in the simultaneous online presence of bidders.

However, if no such functional equivalent is provided in the re-engineered electronic system, or bids are merely opened online (without the simultaneous online presence of bidders), and then subsequently put up for display, or corners are cut for example by not having online countersigning of the opened bids by the TOE-officers in the simultaneous online presence of bidders, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

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.

On-the-Ground Situation in Flawed e-Procurement Implementations: In a very questionable manner, most e-procurement systems have done away with the Online Public-TOE. As mentioned above, in such systems bids no doubt are opened online, but not in the simultaneous online presence of bidders. The procedures of manual tendering which are interactive in nature and conducted in the presence of other bidders, are thereby done away with. After opening, the bid contents may (or may not) be put up for display to the bidders. In either case, it gives rise to the possibility of bid tampering.

Brief Remedial 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 application has comprehensive functionality for a transparent Online Public-TOE. Well established practices of manual tender opening (with legal and transparency related significance) should have corresponding functional equivalents in the electronic system 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 *simultaneous online presence* of 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-TOE.

ii. Security Checks to assure bidders of non-tampering of their bids (during storage), et al during the online TOE itself

iii. One-by-one opening of the sealed bids in the simultaneous online presence of the bidders

iv. Allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of bidders) simultaneous with the opening of that bid. (This would be the functional equivalent of reading out aloud the salient points of each opened bid in the manual system)

v. 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

vi. Digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders

vii. Preparation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders.

For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* (e-Procurement Integrity Matrix, especially sections V (3) and VI (8)); *Reference-2* (e-Procurement Guidelines, Annexure-I, especially sections 5 and 6).

(**Red Flag No.3**): **Most e-procurement systems do not have the functionality to accept 'encrypted (ie sealed) detailed bids'**.

<u>Background</u>: In the manual process of bidding or tendering, for example in a single-stage-two-envelope tender, both the technical bid-part and the financial bid-part are separately sealed in paper-envelopes to ensure 'confidentiality' of each bid-part.

In the e-procurement system also it is expected that both bid-parts would be encrypted before being submitted.

However, if no such functional equivalent is provided in the re-engineered electronic system, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: 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' may be encrypted. This is against the established practices of ensuring confidentiality of technical bids.

Brief Remedial Suggestions:

As in the manual tendering process, all bid envelopes, viz technical, financial, and pre-qualification, as applicable 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 (for capturing the summary or salient aspects of a bid, especially those which are typically read out during the public TOE in the manual system), as well as, an accompanying detailed bid (which could be a large file). All bid parts must be encrypted and digitally signed. If required, printed brochures, manuals, physical samples etc can be submitted offline.

For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* (e-Procurement Integrity Matrix, especially sections II (3) and VI (6,7); *Reference-2* [e-Procurement Guidelines, Annexure-I (especially sections 1.2, 6.1, 6.2) and Annexure-III].

(**Red Flag No.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.**

Background: In the manual process of bidding or tendering, a bidder signs every page of the bid being submitted. This is for ensuring authenticity of each page of the document being submitted. Also, any subsequent change in the document (in the form of erasure or over-writing) has to be authenticated with signature of the bidder otherwise the change is unauthorized or can be the result of tampering. The need for a similar process is certainly not obviated in the e-procurement system. Unauthorized changes in an electronic document will not even be visible to the eye, unless adequate precautions have been taken.

A re-engineered functional equivalent of the physical signatures on a paper document can be the use of Digital-Signatures (based on PKI, or Private-Key-Public-Key pair). With proper implementation, a digitally signed electronic document can establish three things about the signed data– *authenticity*, *non-repudiation* and *integrity*. With proper implementation, the integrity aspect establishes the non-tampering of the electronic document.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

<u>On-the-Ground Situation in Flawed e-Procurement Implementations</u>: Some e-procurement systems do not use digital signatures at all. Some systems use it for only signing the bids. Some systems have facility for limited signing but corresponding facility for verification is missing, thus making the act of signing effectively useless.

To justify as to why they are not using digital signatures, 'misconceptions' are often propagated by vested interests (or out of ignorance) about the use of digital signatures. Some of these misconceptions are outlined below.

Misconception	**Clarification**
Digital signatures are expensive	It is incorrect to say that digital signature certificates are expensive. Cost has to be seen with reference to the context. Where tenders of value running into millions of USD (or even tens of thousands of USD) are involved, a bidder should not mind spending the equivalent of USD 10 to 30 for a digital certificate which will last him for a year or two. This would be equivalent to the cost of going by a cab from one's office to another office in the same city! The same certificate can also

	be used for other purposes.
Digital signatures cannot be used from web-cafes	This is incorrect. There is no technical constraint in the use of digital signatures from web-cafes.
For a foreign bidder (ie potential offshore supplier) to acquire digital signatures from the country of the procuring-entity, he has to travel to the country of the procuring entity	This is certainly not true for a country like India. The position can be checked for other countries. There are well established procedures, at least in India, for a foreign supplier's representative to get a certificate without travelling to India.
User id and password can be as robust and reliable as any other method, including PKI	PKI-based digital signatures are being used for one or all of the following purposes/ functions: a) To 'login' to e-GP portal/ application b) To establish the identity of the signatory of the electronic record/ document (eg an electronic bid, or bidding-documents) c) To sign the 'content/ data' of the electronic record/ document (eg an electronic bid, or bidding-documents) d) To protect against 'tampering' of the electronic record/ document (eg an electronic bid, or bidding-documents) , ie ensuring its 'integrity' While other forms of electronic authentication (or electronic signatures) such as 'only password' (user id normally being a common factor) may achieve purpose 'a' mentioned above (with possibly lower security than PKI), it certainly cannot address other purposes mentioned above, and certainly not the aspect relating to non-tampering.
The UNCITRAL Convention (2006) considers other forms of electronic authentication equal to digital signatures	There are riders in the UNCITRAL Convention, and unless these are understood, misleading conclusions will be drawn. Furthermore, it may please be noted here that use of digital signatures is not just for the

	purpose of authentication. It also serves a very important role for establishing the 'integrity' (ie non-tampering) of electronic records. For example, while Biometrics may be considered as an alternative method of authentication, it would not serve the purpose in respect of ensuring integrity of electronic records.

Brief Remedial Suggestions:

Use of digital signatures must be as per the letter and spirit of the IT Act 2000 (*Reference-4*) 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, 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.

For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* (e-Procurement Integrity Matrix, especially section V; *Reference-2* (e-Procurement Guidelines, Annexure-I, especially section 5, and Annexure-IV).

(**Red Flag No.5**): **In most e-procurement systems, functionality of the system is limited** [eg **all types of bidding methodologies are not supported**].

Background: In the manual process of bidding or tendering, depending on the circumstances and nature of a tender, one of the many bidding methodologies may be prescribed by a procuring entity, and the bidder would have to respond accordingly. These methodologies could include the following:

a) Single-stage, single-envelope

b) Single-stage, two-envelope
c) Two stage (with facility for 'technical conformance', and if required, 'revised tender documents')
d) Two-stage, two-envelope
e) Where required, the above may be combined with a Pre-qualification stage
f) In some cases, the procuring entity may allow submission of one or more alternative-bids
g) Each bid part (eg technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file.
h) After having submitted the 'original' bid for each bid-part, a bidder has a right to submit:
- 'Modification' bid
- 'Substitution' bid
Or 'Withdrawal' bid for all his bid-submissions.

An e-procurement/ e-tendering system should provide the functional equivalent of the above methodologies.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

<u>On-the-Ground Situation in Flawed e-Procurement Implementations</u>: In some e-procurement systems, only 'single-stage-single-envelope' bidding is supported, which may be good enough only for stores items. 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, and at best such systems offer partial functionality.

<u>Brief Remedial Suggestions</u>:

The e-tendering system should support all established bidding methodologies. Depending upon the requirements of a tender any one of the multiple bidding methodologies as outlined below may be used:

- 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
- Pre-qualification stage, where required
- Where required, submission of one or more alternative-bids, as applicable
- Each bid part (eg 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
- After having submitted the 'original' bid for each bid-part, a bidder should have the facility to submit:
  - 'Modification' bid
  - 'Substitution' bid

  Or 'Withdrawal' bid for all his bid-submissions.

The e-tendering/ e-procurement 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).

For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* (e-Procurement Integrity Matrix, especially sections VI (6); *Reference-2* (e-Procurement Guidelines, especially sections '1.2, 3.1, Annexure-I (sections 1.2, 5.1, 6.1), Annexure-II, Annexure-III).

(**Red Flag No.6**): **Many e-procurement systems are such that it results in abdication of powers of the concerned officers of the Government Procuring Entity.**

Background: In the manual process of bidding or tendering in a large Government or public-sector procuring entity, there can be multiple indenting departments, multiple tendering authorities (ie entities which can invite tenders in their name), and tens (and sometimes hundreds) of officers involved with different activities relating to various tenders.

A re-engineered functional equivalent of the above administrative hierarchy is required if the concerned officers of the Government procuring entity are to perform their duties without abdicating their powers to others.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations:

In many e-procurement/ e-tendering systems, the concerned departments and officers are not able to themselves execute their duly assigned roles as in the manual process, and are constrained to re-assign/ abdicate their roles and responsibilities to a few tech-savvy technicians or the personnel of the service-provider of the e-tendering system.

Furthermore, in some situations this also 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 (*Reference-4*), and equivalent provisions, para 3(b) of Article-6 of the UN Model Law (*Reference-5*).

Brief Remedial Suggestions:

Changing over to e-procurement does not imply that the powers and duties (including those under the Official Secrets Act) of the officers for the core tendering processes can be passed on to ‘third-party service providers’, or to a few technical personnel within the procuring entity. Each officer, who currently enjoys powers and has responsibilities relating to 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.

For a more detailed explanation of the issues, the reader may refer to -- a) *Reference-1* [e-Procurement Integrity Matrix, especially sections V (1, 2) and VII (7); *Reference-2* (e-Procurement Guidelines, especially Annexure-I, (section 5.1)].

Note-4: The Red Flags described above essentially relate to the design and functionality of the e-procurement application. The two red-flags described below are not directly related to the core e-procurement application. However these are important allied concerns.

(**Allied Red Flag No. i**): **Diluting the Focus on Security, Transparency and Functionality of the core e-Procurement System by diverting attention to Integration with Backend ERP/ other Financial Systems**:

Background:

The prime objective of e-procurement strategy should be to first build secure, transparent e-procurement systems with all the required vital functionality. Once this is achieved, additional advantages can be gained through integration with back-end ERP/ Financial systems. This is important as approximately 80% of the public expenditure is through tenders which constitute less than 20% in number (Large-Value-Small-Number tenders). On the other hand, tenders which constitute less than 20% in value, make up for more than 80% in number (Low-Value-Large-Number tenders, or e-Purchasing). Because of the smaller number of ‘Large-Value tenders’, the existing financial systems are reasonably equipped to handle the financial record keeping part. Integration with backend ERP/ Financial systems would predominantly streamline ‘e-Purchasing’ which constitutes less than 20% of public procurement in value-terms, and is anyway not an area of major scams.

On-the-Ground Situation in Flawed e-Procurement Implementations: In some countries, without first strengthening and stabilizing the core e-procurement system(s), the attention is being diverted to integration with ERP/ Financial systems. In the process, the core e-procurement system(s) have very rudimentary security and transparency related functionality. This trend can prove risky in the sense that it can jeopardize the stated principles of public procurement, and compromise security and transparency.

Brief Remedial Suggestions:

Use of rudimentary e-procurement modules of ERP systems, or integration of rudimentary e-procurement applications with back-end ERP/ Financial systems should be avoided.

Integration with back-end ERP/ Financial systems can be taken up once the main e-procurement system(s) have stabilized.

If integration with backend ERP/ Financial systems is necessary, it must be ensured that there is no compromise whatsoever in the security, transparency related functionality and robustness of the core e-procurement system.

(**Allied Red Flag No. ii**): **Misconceptions and Myths about Certified and Tested e-Procurement Systems**

Background: Many e-procurement systems with weak functionality try to cover-up their vulnerabilities by using the following as a fig-leaf :

- Obtaining Certification for Security Tests like -- CERT, OWASP, FBI Top 20, etc
- Obtaining Certifications like -- ISO 27001 et al

While the above tests are important and useful, these are *not sufficient*. These tests are general in nature, and do not have anything specific to address the intricacies of e-procurement.

Furthermore, customization invalidates any previous certification. If e-procurement software is customized for each project, the above mentioned general security tests performed on some previous version of the software, lose their relevance.

Brief Remedial Suggestions:

a) 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'.

b) Government of each country which is planning to adopt e-procurement should prepare detailed guidelines similar to the documents referred to herein as *Reference-1* and *Reference-2*.

c) Government of each country should empower a department under their Ministry of Information Technology or equivalent to conduct 'e-procurement functionality and security related tests' as referred to in the *Referenc-2* document.

REFERENCES

1. "e-Procurement Integrity Matrix". (2010). Transparency International India (TII).
   URL: http://transparencyindia.org/integrity_matrix.php

2. "e-Procurement Guidelines." "Guidelines for Compliance to Quality Requirements of eProcurement Systems." (2011, August 31). Department of Information Technology, Government of India.
   URL: http://egovstandards.gov.in/guidelines/guidelines-for-e-procurement/e-Procurement%20Guidelines.pdf/view

3. Schneier, Bruce. (1996-2006). "Applied Cryptography." John Wiley & Sons, Inc.

4. "Information Technology Act 2000." Government of India.

5. "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001." United Nations.

(**Jitendra Kohli** can be contacted at:

jkohli@electronictender.com)

ANNEXURE-I

Typical Broad Steps in Government Tendering conducted manually (which are expected to have electronically conducted equivalents in an e-Procurement System):

(Buyer Perspective)

- □ Requisition/ Indent Approval
- □ Advertisement of Bid-Invitation/ Tender Notice/ Notice Inviting Tender (NIT)
- □ Advertisement of Corrigenda, ie amendments to a Tender Notice
- □ Sale/ Distribution of Tender Documents
- □ Distribution of Addenda, ie amendments to Tender Documents
- □ Responding to Clarification to Tender Documents/ Pre-Bid Meeting
- □ Receipt and secure Storage of Sealed-Bids
- □ Conducting a transparent Public Tender Opening Event (TOE). Some salient steps in a transparently conducted TOE include:

a) Authorized representatives of bidder organizations who have submitted their bids are entitled to be present and have to sign in their attendance.

b) Each bid is opened one at a time in front of the participating bidders, and the concerned bidder is entitled to satisfy himself that his bid packet is intact and has not been tampered with.

c) If Bid security [earnest money deposit (EMD)] is applicable for a tender, then details of the EMD submitted, or exemption claimed with basis thereof is disclosed to the participants.

d) Salient points of each opened bid are read out aloud for the benefit of the participating bidders, and to ensure that no change is made in the bid contents later through connivance. Participating bidders take notes of the competitors' bid contents which are being read out.

e) Clarifications may be sought from a bidder whose bid has been opened and record is made of the query and the response.

f) Each page of the opened bid is countersigned during the TOE itself (by each tender opening officer (typically up to 3) to ensure that no change is made in the bid contents later through connivance.

g) After all the bids are opened and countersigned by the TOE-officers, the minutes of the meeting (ie TOE) are to be recorded.

h) Each bid part may be opened in a separate tender opening event in which only the authorized bidders are allowed. This is supposed to be done in a very transparent manner with proper scheduling of events and proper information to the concerned bidders.

i) Bid parts which are due for opening in a subsequent tender opening event are securely stored till that event.

j) If in a particular TOE, if it is decided not to open the bid of a bidder, then such bids are returned opened.

□ Evaluation of Bids and seeking Technical Conformance/ Clarifications, where relevant

□ Receipt and secure Storage of Sealed Revised Bids, where relevant

□ Follow-on Public Tender Opening Event(s) , where relevant

□ Award of Contract

(Supplier Perspective)

□ Searching/ Viewing advertisement of Bid-Invitation/ Tender Notice/ NIT

□ Searching/ Viewing advertisement of Corrigenda

□ Procurement/ Receipt of Tender Documents

□ Receipt of Addenda

□ Seeking Clarification to Tender Documents

□ Preparation and Submission of Sealed-Bids

□ Attending Public Tender Opening Event (related activities are already covered under 'Buyer Perspective'.

□ Responding to Clarifications sought by Buyer, where relevant

□ Preparation and Submission of Revised Sealed-Bids, where relevant

□ Attending follow-on Public Tender Opening Event(s) , where relevant

□ Receipt of Award (or regret)

ANNEXURE - II

Salient Benefits of e-Procurement

- ■ Summary of 'Overall' Benefits of e-Procurement to a Buyer Organization

- ➢ Reduction in Time
- ➢ Reduction in Cost
- ➢ Reduction in Tedium
- ➢ Wider Reach
- ➢ Enhanced Security (Conditional)
- ➢ Increased Transparency (Conditional)
- ➢ Availability of Supplier Profiles
- ➢ Enhanced Choice of Vendors/ Suppliers (Increased Competition)
- ➢ Streamlining of the Procurement Processes (Conditional)
- ➢ Should get Better Prices because of reduced overheads of Suppliers
- ➢ Assists the top-management in ensuring better Control over the procurement activities of the organization with minimal physical intervention (Better Control with enhanced Accountability) [Conditional]
- ➢ Choice and combination of bidding methodologies, including sealed-bid e-procurement methodologies, combined with e-ReverseAuction methodologies for betterment of prices [Conditional]

- ■ Summary of 'Overall' Benefits of e-Procurement to a Supplier Organization

- ➢ Reduction in Time

- Reduction in Cost
- Reduction in Tedium
- Wider Reach
- Enhanced Security (Conditional)
- Increased Transparency (Conditional)
- Availability of Buyer Profiles
- Streamlining of the processes for participating in tenders (Conditional)
- Assists the top-management in ensuring better Control over the bidding activities of the organization with minimal physical intervention (Better Control with enhanced Accountability) [Conditional]
- Extended opportunity to win a bid in a transparent manner, in cases where the Purchase organization resorts to e-ReverseAuction after the electronic sealed-bid round [Conditional]