TelegraphicAddress :
"SATARKTA: New Delhi

E-Mail Address
cenvigil@nic.in

Website
www.cvc.nic.in

EPABX
24651001 - 07

फैक्स/Fax : 24616286

सं. / No. No. 009/VGL/002

भारत सरकार
केन्द्रीय सतर्कता आयोग
GOVERNMENT OF INDIA
CENTRAL VIGILANCE COMMISSION

सतर्कता भवन, जी.पी.ओ. कॉम्पलैक्स,
ब्लॉक-ए, आई.एन.ए., नई दिल्ली-110023
Satarkta Bhawan, G.P.O. Complex,
Block A, INA, New Delhi 110023

CVO Dy. No. 2070/2010 Date 13/5/2010

दिनांक / Dated 26th April, 2010

Circular No 18/04/2010

Subject: - Implementation of e-tendering solutions – check list.

Guidelines were prescribed in this office OM of even number, dated 17.09.2009, on the above-cited subject, advising organisations to take due care to see that effective security provisions are made in the system to prevent any misuse. It has been observed during security audit carried by CTEO that e-procurement solutions being used by some of the organisations lack security considerations as envisaged in the Commission's guidelines dated 17.09.2009. Some of the shortcomings / deficiencies are of repetitive nature.

A check list to achieve security considerations in e-Procurement solutions is enclosed for information. Organisations concerned may follow the same while implementing e-tendering solutions to address the security related concerns.

(V. Ramachandran)
Chief Technical Examiner

To

All CVOs of Ministries/Departments/PSUs/Banks/Insurance Companies/
Autonomous Organisations/Societies/UTs.

CHECK POINTS TO ACHIEVE SECURITY CONSIDERATIONS IN E-PROCUREMENT SOLUTIONS

S.N.	SECURITY CONSIDERATIONS	Please Tick ✓	
1.	Whether the application is secure from making any temporary distortion in the electronic posting of tender notice, just to mislead certain vendors?	Yes	No
2.	If yes at 2 above, then whether any automatic systems alert is provided in the form of daily exception report in the application in this regard?	Yes	No
3.	Whether application ensures that the tender documents issued to / downloaded by bidders are complete in shape as per the approved tender documents including all its corrigendum?	Yes	No
4.	Is there any check available in the application to detect & alert about the missing pages to the tenderer, if any?	Yes	No
5.	Whether application ensures that all the corrigendum issued by the Competent Authority are being fully communicated in proper fashion to all bidders including those who had already purchased / downloaded the bid documents well ahead of the due date & before uploading the corrigendum?	Yes	No
6.	Whether system is safe from sending discriminatory communication to different bidders about the same e-tendering process?	Yes	No
7.	Whether e-procurement solution has also been customised to process all type of tenders viz Limited / Open / Global Tenders?	Yes	No
8.	Whether online Public Tender opening events feature are available in the application?	Yes	No
9.	Whether facilities for evaluation / loading of bids, strictly in terms of criteria laid down in bid documents are available in the application?	Yes	No
10.	Whether sufficient safeguards have been provided in the application to deal with failed attempt blocking?	Yes	No
11.	Whether application is safe from submission of fake bids?	Yes	No
12.	Whether encryptions of bids are done at clients end?	Yes	No
13.	Whether safety against tampering and stealing information of submitted bid, during storage before its opening, is ensured?	Yes	No
14.	Whether application is safe from siphoning off and decrypting the clandestine copy of a bid encrypted with Public key of tender opening officer?	Yes	No
15.	Whether application is safe from mutilation / sabotage or otherwise rendering the encrypted bid in the e-tender box during storage, to make it unreadable / invalid in any form, before opening of the bids?	Yes	No

16.	Whether introduction of special characters / executable files etc by users are restricted in the application?	Yes	No
17.	Whether validity check of DSC is being done at server end?	Yes	No
18.	Whether system supports the feature that even though if a published tender is being deleted from the application, system does not allow permanent deletion of the published tender from the Database?	Yes	No
19.	Whether sufficient security features are provided in the application for authentication procedure of the system administrator like ID, password, digital signature, biometric etc?	Yes	No
20.	Whether audit trails are being captured in the application on media not prone to tampering, such as optical write once?	Yes	No
21.	Whether log shipping feature is available, where a separate dedicated server receives the logs from the application over a web service in real time?	Yes	No
22.	Whether integrity and non-tampering is ensured in maintaining the server clock synchronisation & time stamping?	Yes	No
23.	Whether application generates any exception report / system alerts etc to indicate the resetting of the clock, in case the application for time stamping is killed at the server level and time is manipulated?	Yes	No
24.	Whether application ensures that the quotes from various bidders with their name are not being displayed to any one including to the Organisation during carrying out of the e-reverse auctioning process?	Yes	No
25.	Whether application is fit for usage complying with the requirements of tender processing viz Authenticity of tenderer, non-repudiation and secrecy of information till the actual opening of tenders.	Yes	No
26.	Whether any comprehensive third party audit [as per statutory requirement and also as per the requirements of e-tender processing (compliance to IT Act 2000)] was got conducted before first putting it to public use?	Yes	No
27.	Whether application complies with the Commission's Guidelines dated 17.09.2009 on Security considerations for e-procurement Systems.	Yes	No