Telegraphic Address :
"SATARKTA" New Delhi

E-Mail Address :
cenvigil@nic.in

Website
www.cvc.nic.in

EPABX
24651001 - 07

फैक्स/Fax : 24616286

सं. / 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

दिनांक / Dated..............................
17th September, 2009

Circular No 29/9/09

Subject : - Implementation of e-tendering solutions.

Guidelines were prescribed in this office OM of even number, dated 13/01/2009, on the above-cited subject, advising organisations to follow a fair, transparent and open tendering procedure, to select the application service provider for implementing their e-tendering solutions.

2. It is clarified that while ensuring fair play, transparency and open tendering procedure for e-tendering solutions, the organisations must take due care to see that effective security provisions are made in the system to prevent any misuse. In this regard, the guidelines on security related issues in e-tendering systems are enclosed for information. Organisations concerned may follow these guidelines while implemeting e-tendering solutions to contain the security related loop holes.

Ramachandran
(V. Ramachandran)
Chief Technical Examiner

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

Guidelines on Security considerations for e-procurement System.

1.0 E-procurement Systems.

E-procurement provides a platform for the collaborative procurement of goods, works and services using electronic methods at every stage of the procurement process. The e-procurement platform transacts confidential procurement data and is exposed to several security threats. Agencies World over face threats to their online e-procurement platforms and the same are addressed by employing a combination of security features and security best practices which result in reduced threat of data loss, leakage or manipulation.

2. Security of e-Procurement system.

2.1 Security of e-procurement system is essentially an amalgamated output of Security of Infrastructure, Application and Management. Assuming the management issues are taken care of the following aspects of Infrastructure and Application are essential to have a fairly secure e-Procurement.

2.2 Security Infrastructure level:

Issues	Best Practices to achieve security considerations
Perimeter Defence.	Deployment of routers, Firewalls, IPS/IDS, Remote Access and network segmentation.
Authentication.	Network authentication through deployment of password policy for accessing the network resources. To minimize unauthorised access to the e-procurement system at system level.
Monitoring	Deployment of logging at OS/ network level and monitoring the same.
Secure configuration of network host.	The security of individual servers & workstations is a critical factor in the defence of any environment, especially when remote access is allowed. Workstations should have safeguards in place to resist common attacks.
System patching.	As the vulnerability of the system are discovered almost regularly and the system vendors are also releasing the patches. It is expected the host are patched with latest security updates released by the vendors.
Control of malware.	Suitable control like anti-virus, anti spyware ext. should be deployed on the host associated with e-procurement system. However, option for running the services at non-privileged user profile may be looked for. Otherwise,

	suitable operating system which is immune to virus, trojan and malware may be deployed.
Structured cabling.	The availability of the network services is critically dependent on the quality of interconnection between the hosts through structured including termination and marking. It is expected the e-procurement system has implemented structured cabling and other controls related with network and interconnection.

2.3 Security at Application level.

2.3.1 Security during design.

Issues	Best Practices to achieve security considerations
Authentication	The authentication mechanism of the e-procurement application should ensure that the credentials are submitted on the pages that are server under SSL.
Access Control.	The application shall enforce proper access control model to ensure that the parameter available to the user cannot be used for launching any attack.
Session management.	The design should ensure that the session tokens are adequately protected from guessing during an authenticated session.
Error handling.	The design should ensure that the application does not present user error messages to the outside world which can be used for attacking the application.
Input validation.	The application may accept input at multiple points from external sources, such as users, client applications, and data feeds. It should perform validation checks of the syntactic and semantic validity of the input. It should also check that input data does not violate limitations of underlying or dependent components, particularly string length and character set. All user-supplied fields should be validated at the server side.
Application logging and monitoring.	Logging should be enabled across all applications in the environment. Log file data is important for incident and trend analysis as well as for auditing purposes. The application should log failed and successful authentication attempts, changes to application data including user accounts, serve application errors, and failed and successful access to resources.

	When writing log data, the application should avoid writing sensitive data to log files.

2.3.2 Security during application deployment and use.

Issues	Best Practices to achieve security considerations
Availability Clustering. Load balancing.	Depending on the number of expected hits and access the options for clustering of servers and load balancing of the web application shall be implemented.
Application and data recovery.	Suitable management procedure shall be deployed for regular back-up of application and data. The regularity of data backup shall be in commensurate with the nature of transaction / business translated into the e-procurement system.
Integrity of the Application. Control of source code. Configuration management.	Suitable management control shall be implemented on availability of updated source code and its deployment. Strict configuration control is recommended to ensure that the latest software in the production system.

2.3.3 Security in Data storage and communication.

Issues	Best Practices to achieve security considerations
Encryption for data storage.	Sensitive data should be encrypted or hashed in the database and file system. The application should differentiate between data that is sensitive to disclosure and must be encrypted, data that is sensitive only to tampering and for which a keyed hash value (HMAC) must be generated, and data that can be irreversibly transformed(hashed) without loss of functionality (such as passwords). The application should store keys used for decryption separately from the encrypted data. Examples of widely accepted strong ciphers are 3DES, AES, RSA, RC4 and Blowfish. Use 128-bit keys(1024 bits for RSA) at a minimum.
Data transfer security.	Sensitive data should be encrypted prior to transmission to other components. Verify that intermediate components that handle the data in clear-text form, prior to transmission or subsequent to receipt, do not present an undue threat to the data. The application should take advantage of

	authentication features available within the transport security mechanism. Specially, encryption methodology like SSL must be deployed while communicating with the payment gateway over public network.
Access control.	Applications should enforce an authorisation mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. Role-based access controls should be enforced at the database level as well as at the application interface. This will protect the database in the event that the client application is exploited. Authorisation checks should require prior successful authentication to have occurred. All attempts to obtain access, without proper authorisation should be logged. Conduct regular testing of key applications that process sensitive data and of the interfaces available to users from the Internet Include both "black box" informed" testing against the application. Determine if users can gain aces to data from other accounts.

3.0 Some of the other good practices for implementers of e-procurement to achieve security considerations are as follows:-

3.1 Common unified platform for all department.

A single platform to be used by all departments across a State / Department / Organisations reduces the threat to security of data. With a centralised implementation, where in the procurement data is preferably hosted and maintained by the State / Department / Organisations itself, concerns of security and ownership of data are well addressed. A common platform further facilitates demand aggregation of common items across State / Department / Organisations, and result in economies of scale.

3.2 Public key Infrastructure (PKI) Implementation

This is one of the most critical security features that are required to be implemented in order to establish non-repudiation and to ensure the security of the online system. Under the system, participating contractors and suppliers, as well as the departmental users, are issued a Digital Signature Certificate (DSC) by a licensed Certification Authority.

3.3 Third Party Audit.

It is recommended that the implemented solution be audited by a competent third party at-least once a year.

Through the above-mentioned steps, the complete security of the system and the transacted data can be ensured and may be communicated to all concerned agencies.