KIOCL LIMITED

Vigilance Department

VIGILANCE NEWSLETTER

JULY 2022

Vigilance Newsletter
JULY 2022

Vigilance department wishes all the employees and their families a very Happy Eid-ul-Zuha, Independence Day, Gauri-Ganesha puja, Sri Krishna Janmashtami and Onam, in advance.

Continuing the efforts of Vigilance Department to help the Company and its employees to stay abreast of the changing methods of working and adapting to them while maintaining high level of integrity, this issue of Vigilance Newsletter brings the latest circulars and notifications issued by various Departments of Government of India having bearing on our working and vigilance.

This issue also has write-up on the fundamentals to be observed in E-Procurement and associated E-Vigilance. Case studies of system improvements implemented in different CPSEs is being shared which can be emulated by KIOCL.

I expect that this edition would enhance our understanding of relevant subjects and help in our working

1st July, 2022 Chief Vigilance Officer

Contents

Circular/Notifications/Guidelines issued by GoI

Systemic Improvements and Preventive Vigilance initiatives

Articles on E-Procurement, E-Procurement through GeM and E-Vigilance

Objective Assessment of Capacity and Capability of Bidders in Power Grid Corporation of India Ltd (POWERGRID)

1. BRIEF DESCRIPTION OF THE MEASURE/ INITIATIVE

A measure of systems improvement facilitating the elimination of subjectivity in tender awards through the incorporation of event-based eligibility/disqualification clauses in Bid documents and dispensation of post-bid performance evaluation of existing contractors in ongoing projects. As part of tender evaluation, assessment of capacity and capability of bidder to perform the contract was earlier carried out as per the following pre-defined eligibility criteria:

MAAT (Minimum Average Annual Turnover)

Manufacturing Capacity

Balance Bid Capacity

Further, performance review of existing contractors in ongoing projects was also being done earlier through a standing committee.

In order to make the performance review of any agency more objective, transparent, and fair, POWERGRID vigilance emphasized that any performance assessment mechanism involving on-going contracts with bearing on fresh tenders at the post-bid stage ought to be avoided as far as possible.

Bid documents were accordingly standardized by POWERGRID with approval of the Board of Directors based on Vigilance suggestion to incorporate a filtering mechanism to exclude bids from non-performers/ poor performers/ saturated performers based on objective eligibility parameters.

Towards this end, the following critical negative events have now been incorporated as parameters for deciding the eligibility/ineligibility of a bidder and these form part of the Bid document:

Termination of contract due to Contractor's default and encashment of Performance Guarantee due to non-performance;

Repeated failure of major types of equipment while in service;

Substantial portion of works (more than 50% of the contract) is sub-contracted, under the existing Contract;

Firm has been referred to NCLT under Insolvency and Bankruptcy Code.

2. BACKGROUND

Earlier the assessment of capacity and capability of bidders was done on the predefined eligibility criteria of MAAT (Minimum Average Annual Turnover), Manufacturing Capacity, and Balance Bid Capacity. The Balance Bid Capacity was earlier defined as follows:

Balance Bid Capacity = 3T– B, where T= Maximum value of works executed in any one financial year during the last 5 financial years taking into account the completed as well as the works in progress. B= Value of existing commitments and ongoing similar works yet to be completed

Declaration to be given by Bidder in his bid.

Bidder's balance bid capacity was checked during the first stage evaluation (before price bid opening) considering his declaration as well as other packages under award and zone of consideration.

In addition to the above, a performance review of existing contractors in ongoing projects was also being done by a standing committee based on inputs from the site and various other departments. Subsequently, Vigilance advised that appropriate measures for systemic improvement in this regard may be put in place to avoid post-bid subjectivity in evaluation of bidders and to bring in transparency by introducing pre-defined events.

3. IMPLEMENTATION

Amendment to the existing procedure of assessment was notified on 17.01.2020 duly approved by the Board of Directors of POWERGRID. It is now fully implemented across the Company and is applicable to all tenders.

4. IMPACT AND BENEFITS

Bid-exclusion process is now devoid of subjectivity and administrative discretion. The same is based on event-based parameters that are clearly spelt out in Bid documents. It is also a measure to arrest the setbacks/delays, if any, in ongoing contracts more efficiently and to decide eligibility/ineligibility of bidders for award of new contracts before the opening of Financial Bids.

5. POTENTIAL FOR REPLICABILITY

The new guidelines for the assessment of capacity and capability introduced in POWERGRID can be suitably implemented in tendering in the award of works by the majority of organizations.

System for Allocation of Vendor Code and Digital Signatures in BEML

1.0 BRIEF DESCRIPTION OF THE MEASURE/ INITIATIVE

To avoid creation of fake Vendor account and to streamline the allocation of Vendor Code and Digital Signatures, various measures/ steps have been undertaken:

- Allocation of Vendor Codes only if request is received from authorized email of Vendor.

- Vendor User-ID and Password should be intimated only to Vendor and not to Purchase Officers.

- Changes in the Vendor database only on the vendor request through his authorized email ID or Company Letter head.

- Maintenance of Centralized Database with respect to all of the digital Signatures by Corporate IT team.

- Surrendering of digital signature by Purchase officer on transfer before relieving order.

- No sharing of Digital Signature allotted for approving bids.

2.0 BACKGROUND

Prior to implementation of this system, allocation of vendor code was done by IT Team on receipt of e-mail from any source including the e-mail from Purchase officers. This posed a serious risk of creation of fake Vendor accounts and collusion of Vendors with Purchase Officers. To avoid the same, a study was carried out and some certain measures have been taken and necessary changes have been implemented in SRM portal for e-tendering.

3.0 IMPLEMENTATION

Necessary modification in SAP Master Data and SRM portal for e-tendering has been carried out and system has been implemented all across in BEML.

4.0 IMPACT AND BENEFITS

- Transparency & fair play, avoiding fraud in bidding process.

- Maintenance of Vendor Master

- Increased transparency in SRM portal of e-tendering

5.0 POTENTIAL FOR REPLICABILITY

The new system for Allocation of Vendor Code and Digital Signatures introduced in BEML can be suitably implemented by all the CPSEs.

Electronic Procurement (e-Procurement)

1.0 What is Electronic Procurement (e-procurement)

i) Electronic Procurement (e-Procurement) is the use of information and communication technology (specially the internet) by the Procuring Entity in conducting procurement processes with the vendors/ contractors for the acquisition of goods (supplies), works and services aimed at open, non-discriminatory and efficient procurement through transparent procedures. As per GFR 2017, it is now mandatory for Ministries/ Departments to receive all bids through e procurement portals in respect of all procurements.

ii) Ministries/ Departments which do not have a large volume of procurement or carry out procurements required only for day-to-day running of offices and also have not initiated e-procurement through any other solution provider so far may use e-procurement solution developed by NIC. Other Ministries/ Departments may either use e-procurement solution developed by NIC or engage any other service provider following due process.

iii) These instructions will not apply to procurements made by Ministries/Departments through DGS&D rate contracts or Government E-Markets (GeM).

iv) In individual cases where national security and strategic considerations demands confidentiality, Ministries/ Departments may exempt such cases from e-procurement after seeking approval of concerned Secretary and with concurrence of Financial Advisers.

v) In case of tenders floated by Indian Missions abroad, Competent Authority to decide the process of tender and may exempt such case from e-procurement.

2.0 Service Provider

A service provider is engaged to provide an e-procurement system covering the following:

i) All steps involved, starting from hosting of tenders to determination of techno-commercially acceptable lowest bidder, are covered;

ii) The system archives the information and generates reports required for the management information system/ decision support system;

iii) A helpdesk is available for online and offline support to different stakeholders;

iv) The system arranges and updates the Digital Signature Certificate (DSC) for departmental users; and

v) Different documents, formats, and so on, for the e-procurement systems are available.

3.0 Process

In e-procurement, all processes of tendering have the same content as in normal tendering and are executed, once the necessary changes have been made, online by using the DSC as follows:

i) Communications: Wherever traditional procedures refer to written communication and documents, the corresponding process in e-procurement would be handled either fully online by way of uploading/ downloading/ emails or automatically generated SMSs or else partly online and partly offline submission. It is advisable to move to full submissions online. More details would be available from e-procurement service provider's portal. In e-procurement, the tender fee, EMD and documents supporting exemption from such payments are submitted in paper form to the authority nominated in the NIT, but scanned copies are to be uploaded – without which the bid may not get opened. In future, such payments may be allowed online also;

ii) Publishing of tenders: Tenders are published on the e-procurement portal by authorised executives of Procuring Entity with DSC. After the creation of the tender, a unique "tender id" is automatically generated by the system. While creating/ publishing the tender, the "bid openers" are identified – four officers (two from the procuring entity and two from the associated/ integrated Finance) with a provision that tenders may be opened by any two of the four officers. As in case of normal tenders, NITs are also advertised in newspapers and posted on the Procuring Entity website. The downloading of the tender may start immediately after e-publication of NIT and can continue till the last date and time of bid submission. The bid submission will start from the next day of e-publication of NIT. In case of limited and PAC/ single tenders, information should also be sent to target vendors/contractors through SMS/ email by the portal;

iii) Registration of bidders on portal: In order to submit the bid, bidders have to register themselves online, as a one-time activity, on the e-procurement portal with a valid DSC. The registration should be in the name of the bidder, whereas DSC holder may be either the bidder himself or a duly authorised person. The bidders will have to accept, unconditionally, the online user portal agreement which contains all the terms and conditions of NIT including commercial and general terms and conditions and other conditions, if any, along with an online undertaking in support of the authenticity of the declarations regarding facts, figures, information and documents furnished by the bidder online;

iv) Bid submission: The bidders will submit their techno-commercial bids and price bids online. No conditional bid shall be allowed/ accepted. Bidders will have to upload scanned copies of various documents required for eligibility and all other documents as specified in NIT, techno-commercial bid in cover-I, and price bid in cover-II. To enable system generated techno-commercial and price comparative statements, such statements should be asked to be submitted in Excel formats. The bidder will have to give an undertaking online that if the information/ declaration/ scanned documents furnished in respect of eligibility criteria are found to be wrong or misleading at any stage, they will be liable to punitive action. EMD and tender fee (demand draft/ banker's cheque/ pay order) shall be submitted in the electronic format online (by scanning) while uploading the bid. This submission shall mean that EMD and tender fee are received electronically. However, for the purpose of realisation, the bidder shall send the demand draft/ banker's cheque/ pay order in original to the designated officer through post or by hand so as to reach by the time of tender opening. In case of exemption of EMD, the scanned copy of the document in support of exemption will have to be uploaded by the bidder during bid submission;

v) Corrigendum, clarifications, modifications and withdrawal of bids: All these steps are also carried out online *mutadis mutandis* the normal tendering process;

vi) Bid opening: Both the techno-commercial and price bids are opened online by the bid openers mentioned at the time of creation of the tender online. Relevant bidders can simultaneously take part in bid opening online and can see the resultant bids of all bidders. The system automatically generates a technical scrutiny report and commercial scrutiny report in case of the techno-commercial bid opening and a price comparative statement in case of price bid opening which can also be seen by participating bidders online. Bid openers download the bids and the reports/ statements and sign them for further processing. In case of opening of the price bid, the date and time of opening is uploaded on the portal and shortlisted firms are also informed through system generated emails and SMS alerts – after shortlisting of the techno-commercially acceptable bidders;

vii) Shortfall document: Any document not enclosed by the bidder can be asked for, as in case of the traditional tender, by the Procuring Entity and submitted by the bidder online, provided it does not vitiate the tendering process;

viii) Evaluation of techno-commercial and price bids: This is done offline in the same manner as in the normal tendering process, based on system generated reports and comparative statements;

ix) Award of contract: Award of the contract is done offline and a scanned copy is uploaded on the portal. More needs to be done in this regard. The information and the manner of disclosure in this regard must conform to Section 4(1) (b), 4(2) and 4(3) of the RTI Act to enhance transparency and also to reduce the need for filing individual RTI applications. Therefore, the award must be published in a searchable format and be linked to its NIT; and

x) Return of EMD: EMD furnished by all unsuccessful bidders should be returned through an e-payment system without interest, at the earliest, after the expiry of the final tender validity period but not later than 30 (thirty) days after conclusion of the contract. EMD of the successful bidder should be returned after receipt of performance security as called for in the contract.

(This is generic in nature. Procuring Entities may settle and decide the details with the service provider)

****

Source: Manual for Procurement of Works 2019, Ministry of Finance, Department of Expenditure

E-Procurement through Government e-Marketplace (GeM)

Rule 160 of GFR 2017 deals with the e-Procurement process.

An online marketplace (or e-commerce marketplace) is a type of e-commerce site where product or services are offered by a number of sellers and all the buyers can select the product/ services offered by any one of the sellers, based on his own criteria. In an online marketplace, Purchaser’s transactions are processed by the marketplace operator and then product/services are delivered and fulfilled directly by the participating retailers. Other capabilities might include auctioning (forward or reverse), catalogues, ordering, posting of requirements by Purchasers, Payment gateways etc. In general, because online marketplaces aggregate products from a wide array of providers, selection is usually wider, availability is higher, and prices are more competitive than in vendor-specific online retail stores.

Background

Hon'ble Prime Minister, based on recommendations of the Group of Secretaries, decided to set up a dedicated e-market for different goods & services procured by Government Organisations / Departments / PSUs. This meant transforming **DGS&D** into a digital e-commerce portal for procurement and selling of goods and services.

Government e Marketplace (GeM), created in a record time of five months, facilitates online procurement of common use Goods & Services required by various Government Departments / Organisations / PSUs. GeM aims to enhance transparency, efficiency and speed in public procurement. It provides the tools of e-bidding, reverse e-auction and demand aggregation to facilitate the government users, achieve the best value for their money.

Government of India (Allocation of Business) Rules, 1961, vide notification dated 8th December 2017 has made the following entry

- 32. Development, operation and maintenance of National Public Procurement Portal—Government e Marketplace”.

The purchases through GeM by Government users have been authorised and made mandatory by Ministry of Finance by adding a new Rule No. 149 in the General Financial Rules, 2017.

As owner of the National Public Procurement Portal (section 8 Company registered under the companies Act, 2013), GeM SPV builds, operates and maintains the GeM platform, which provides an end-to-end online Marketplace for Central and State Government Ministries / Departments, Central & State Public Undertakings (CPSUs & SPSUs), Autonomous institutions and Local bodies in transparent and efficient manner.

Process

GeM is a one-stop shop for common use goods and services. The procurement process on GeM is end to end from placement of supply order to payment to suppliers. This is to ensure better transparency and higher efficiency. All the process will be electronic and online.

Products and services are listed on GeM by various suppliers as on other e-Commerce portals. The registration of suppliers on GeM is online and automatic based on PAN, MCA-21, Aadhaar authentication etc. The suppliers will offer their products on GeM and the buyer will be able to view all the products as well as compare them. Tools of reverse bidding and e-auction are also available which can be utilised for procurement of bulk quantities.

Demand Aggregation

The best prices to a user can be available if same requirement and demands of various organizations are aggregated. This acts as an incentive for the supplier to quote their best price. For the same products, the demand of various Govt. Departments/PSUs can be clubbed together and reverse auction done on the basis of aggregated demand which will provide the best prices to the Buyer.

Authority of procurement through GeM:

GeM SPV will ensure adequate publicity including periodic advertisement of the items to be procured through GeM for the prospective suppliers. The credentials of suppliers on GeM shall be certified by GeM SPV. The procuring authorities will certify the reasonability of rates. The GeM portal shall be utilized by the Government buyers for direct on-line purchases as under:

i) Up to Rs.50,000/- (Rupees Fifty thousand) through any of the available suppliers on the GeM, meeting the requisite quality, specification and delivery period;

ii) Above Rs.50,000/- (Rupees Fifty thousand) and up to Rs.30,00,000/- (Rupees thirty lakh) through the GeM. Seller having lowest price amongst the available sellers, of at least three different manufacturers, on GeM, meeting the requisite quality, specification and delivery period. The tools for online bidding and online reverse auction available on GeM can be used by the Buyer if decided by the competent authority;

iii) Above Rs.30,00,000/- (Rupees Thirty Lakh) through the supplier having lowest price meeting the requisite quality, specification and delivery period after mandatorily obtaining bids, using online bidding or reverse auction tool provided on GeM;

iv) The invitation for the online e-bidding/reverse auction will be available to all the existing Sellers or other Sellers registered on the portal and who have offered their goods/ services under the particular product/service category, as per terms and conditions of GeM;

v) The above-mentioned monetary ceiling is applicable only for purchases made through GeM. For purchases, if any, outside GeM, relevant GFR Rules shall apply;

vi) The Ministries/Departments/PSUs shall work out their procurement requirements of Goods and Services on either “OPEX” model or “CAPEX” model as per their requirement/ suitability at the time of preparation of Budget Estimates (BE) and shall project their Annual

Procurement Plan of goods and services on GeM portal within 30 (thirty) days of Budget approval;

vii) The Buyers may ascertain the reasonableness of prices before placement of order using the Business Analytics (BA) tools available on GeM including the Last Purchase Price on GeM, Department's own Last Purchase Price; etc.

viii) A demand for goods shall not be divided into small quantities to make piecemeal purchases to avoid procurement through L-1 Buying/bidding/reverse auction on GeM or the necessity of obtaining the sanction of higher authorities required with reference to the estimated value of the total demand. It may be noted that unlike Rate Contracts, the responsibility of reasonableness of rate for procurements from GeM portal does not lie with GeM SPV. It is the responsibility of the Procuring Entity to do due diligence for ensuring reasonableness of rates.

GeM Portal: https://gem.gov.in.

Detailed instructions for user organization registration, supplier registration, listing of products, terms and conditions, online bidding, reverse auction, demand aggregation, call centre, etc. are available on this portal.

Payment Procedure in GeM:

The payment procedure in GeM is governed by O.M. No. F.26/4/2016-PPD dated 26th May, 2016 issued by D/o. Expenditure, M/o. Finance, New Delhi. The salient feature of this O.M. is that it is obligatory to make payments without any delay for purchases made on GeM. The consignee is required to issue an online digitally signed consignee receipt and acceptance certificate after receipt of goods within ten days. Thereafter, the payments are to be released maximum within ten days. The timelines after Consignee Receipt and Acceptance Certificate (CRAC) issued online and digitally signed by consignee will be two (2) working days for Buyer, one (1) working day for concerned DDO and two (2) working days for concerned PAO for triggering payment through PFMS/Government Financial System/Banks for crediting to the supplier's account. Any matter needing a resolution will be escalated to the next higher level in each agency (Buyer, DDO and PAO) where the matter should be resolved within 24 (Twenty-Four) hours in the entire process, payments should not exceed ten days including holidays.

Electronic Reverse Auction (RA)

Electronic Reverse Auction (RA) is a type of auction (classified as dynamic procurement method) where the starting price, bid decrement, duration of auction, maximum number of automatic extensions are announced before start of online reverse auction. If required, RA may be preceded by an e-Procurement stage of eligibility/PQB to shortlist competent bidders who would be allowed to participate in the RA. The shortlisted bidders can after the start of RA start bidding online in an iterative process wherein the lowest bidder at any given moment can be displaced by an even lower bid of a competing bidder, within the duration of the RA. If a new lower bid is received within last few minutes (say two minutes) of closing time, the closing time may get automatically extended by few minutes (say five minutes) for others to respond. Maximum number of such extensions may be stipulated (say five). The most favourable bid at the end of stipulated/extended time is declared as successful. While permitting use of RA, CVC has asked the Departments/organisations to themselves decide on reverse auction for purchases or sales and work out the detailed procedure in this regard. It is, however, to be ensured that the entire process is conducted in a transparent and fair manner.

A Procuring Entity may choose to procure a subject matter of procurement by the electronic reverse auction method, if:

i) Items for Reverse Auction may be selected carefully. Items of strategic, critical and vital nature, items in short supply in market and where there are only a few suppliers are not good candidates for reverse auction.

ii) Items in the nature of commodities, commercially off-the-shelf items, items having large number of suppliers and high value procurements may be more amenable to reverse auction;

iii) It is feasible for the Procuring Entity to formulate a detailed description of the subject matter of the procurement;

iv) There is a competitive market of bidders anticipated to be qualified to participate in the electronic reverse auction, so that effective competition is ensured;

v) The criteria to be used by the Procuring Entity in determining the successful bid are quantifiable and can be expressed in monetary terms;

vi) In cases where pre-qualification of bidders is considered necessary, reverse auction may be carried out after a separate PQB (electronic or otherwise) among the successful bidders only.

Subject to more detailed guidelines in the category-specific manual or other guidelines, the procedure for electronic reverse auction shall include the following, namely:

i) The Procuring Entity shall solicit bids through an invitation to the electronic reverse auction to be published or communicated in accordance with the provisions similar to e-Procurement; and

ii) The invitation shall, in addition to the information as specified in e-Procurement, include details relating to:

a) Access to and registration for the auction;

b) Opening and closing of the auction;

c) Norms for conduct of the auction; and

d) Any other information as may be relevant to the method of procurement. (Rule 167 of GFR 2017)

*****

E-VIGILANCE

INTRODUCTION

What is e-Vigilance?

In normal parlance 'vigilance' means careful attention that we pay to what is happening around us to find out lapses or violations. It connotes watchfulness, prevention and detection of wrongdoings in governance activities. e-Vigilance is a modern tool of watchfulness, prevention and detection by leveraging of modern technology. e-Vigilance ensures compliance of laws, rules and instructions in governance activities by means of inbuilt system of machine intelligence, and thereby detecting violations, if any. It also ensures integrity, transparency and equity in the functioning of Government and public entities which are epitome of good governance.

1.1 BACKGROUND

(a) In this era of technological revolution, it has become possible to deal with complex and diverse government activities in an efficient, transparent, and citizen-centric manner. Over the years, a large number of initiatives have been undertaken by various organizations and authorities of Central and State Governments to usher in an era of e-Governance. Sustained efforts have been made at multiple levels to improve the delivery of services and simplify the processes of accessing them. Use of ICT in India has steadily evolved from computerisation of Organizations to initiatives that encapsulate the finer points of Governance, such as citizen centricity, service orientation, speed, and transparency.

(b) Organizations undertake automation, digitization and digitalization in order to streamline their internal systems, processes to ensure effective customer interface and delivery of seamless services, such as Government to Government (G2G), Government to Citizen (G2C), Citizen to Government (C2G), Government to Business (G2B) and Business to Consumers (B2C) services, etc. The major areas where online systems have made huge impact are e-procurement, e-land records, e-office, e-exams, e-recruitment, e-payments, e-banking, scholarship, life certificate for pensioners, e-subsidies, online booking/reservation (railways, airlines, roadways, etc.), passport services, e-courts and other legal services, medical consultancy, and other IT enabled services.

(c) While digitisation has brought in lots of merits, reducing petty corruptions, efficient delivery of services, improving the quality of life, reduction in time taken for availing services, enhanced transparency, awareness amongst citizens, it poses its own challenges of vulnerability of intentional/unintentional manipulations which need to be diagnosed and tackled on continuous basis. Instances of cyber frauds, cyber-crimes, malpractices by officials and employees of vendors manning the IT systems and outsiders also have come to notice. Apart from the organisations concerned, the Central Vigilance Commission is also receiving/ has received reports/complaints, about incidents of such malpractices.

(d) Organizations should have robust systems and processes of IT based platforms and Vigilance needs to play a pro-active role and to adapt to such organizational changes so that the processes and information in such an environment are within their ambit for scrutiny against vigilance angle or systemic deficiencies. In order to undertake such examination, there is felt need for requisite capacity building in the form of competencies, skills and tools that would help Vigilance examine the data, the reports and the processes.

1.2 ISSUES FACED

Few possibilities to illustrate existing IT systems' susceptibility to corruption and incidents of malpractices are cited below: -

(i) E-procurement/e-tender: There may be instances wherein some bidders could get to know critical information such as bids of the competitors because of inherent infirmities/ vulnerabilities of the system itself and succeed in clinching the tender in their favour. Non-encryption of technical/financial bid and its accessibility is a vulnerability area. Encryption and audit trail/log needs to be ensured. The trails/logs are required to be maintained in such a manner that they cannot be modified/altered by the system administrators.

(ii) E-Recruitment: Delayed publishing of vacancies/recruitment notices on e-platform and actual reduction in e-visibility period of the said notice; additionally, the broken link to open the online form and the system becoming slow/hung in the last few days/hours of the cut off time and non-provision of objection period is an area of concern.

(iii) E-payment – fraud and duping: Numerous cases are reported on a regular basis wherein citizens are duped while making online transactions with various banks and available apps. Payment gets deducted from the account of the customer, but services/goods not delivered and without auto reversal of payment or instant refund. Huge amount of money gets siphoned off in this kind of malpractice. Involvement of employees of the Banking, Financial Services and Insurance (BFSI) sector, outsiders or the employees of the vendor engaged by the BFSI sector partner connivance in incidents/malpractices cannot be ruled out. Given the extensive use of technology in BFSI sector, the risk of unauthorised access, disclosure and modification by unscrupulous employees remains high. Many government schemes now involve Direct Benefit Transfer to the intended beneficiaries. Such kind of e-payment transfers need to be protected from any possible unscrupulous manoeuvring. Pay & allowances to employees, payment to the contractors/ vendors are now made through electronic transfers and are vulnerable to manipulations and frauds. Modification of bank details of intended beneficiaries (for contractual payments, refunds, etc.) should normally not be allowed. If it becomes absolutely necessary (for example in case of closure/merger of banks, etc.) it should be done in a controlled manner, with multi-level approvals, and audit trails.

1.3 PROACTIVE MEASURES TO ENHANCE THE ROBUSTNESS OF THE IT BASED SYSTEMS

(a) E-Systems and processes should be aligned with provisions in the IT Act, Rules and guidelines issued by Ministry of Electronics & Information Technology (MeitY) from time to time.

(b) Relevant SOPs should be put in place by the organizations for strict adherence.

(c) To ensure information security in terms of Confidentiality, Integrity, Availability and Indisputable authentication of ownership of any action (Non-Repudiation), the ICT infrastructure such as E-platforms and IT enabled services comprising of websites, portals, applications, database, user accounts, cloud services, mobile applications, storage devices, Application Program Interfaces (API), encryption mechanisms, etc. are needed. Electronic service environment of the organizations requires to be updated and made robust.

(d) Security Audit: All the IT systems and processes should be security audited by agencies such as STQC or CERT-In empanelled agencies. The software applications, IT system should be tested / audited on regular interval as per the CERT-In guidelines. However, if there is a major change in software application or IT system, then impact of change should be analysed and testing / auditing for security should be done before putting the changed application / IT system in production environment. However, basic details of key personnel of the CERT-In empanelled agencies or any other such organization, like name, Aadhaar number, PAN number, etc. need to be maintained and dynamically updated by CERT-In or any other similarly placed organization.

(e) Information Security Management System: Organizations should have policy which ensures data authorization, process authorization, data safety, non-repudiation, etc. depending upon the need and necessity of the organization. The hiring organization having sensitive and confidential data may exercise due diligence to ensure the integrity of the key personnel of the empanelled agency while getting the security audit done for the organisation.

(f) Ownership and control of the data shall exclusively rest with the concerned public organization.

(g) Maker / Checker Concept: The Agency which has made/supplied the IT systems should not be the Checker of the IT system. The checker should, inter-alia examines the code for the possibility of leakage of confidential data / data loss through malicious code. This should be done for each and every patch that is deployed thereafter.

(h) IT system and its online auditing system should be in separate silos so as to maintain exclusivity of the auditing system. Control of the auditing system should not be with the administrator of the IT system.

(i) Organisations may consider to have backup server(s) placed at a different place other than the primary server(s) where exact replica of the primary server(s) are created on run time basis or at regular intervals as may be decided by the organisation. This will help the organisation recover data in case of any disaster, crashing of primary server, etc.

(j) System of auto generated alert in cases, such as it is becoming slow below a certain level or disruption during submission of bids, application for various services, etc. on the cut-off date and time. A window period for receiving grievances and their redressal should be there.

(k) All transactions should be time stamped with the server clock time. The server time should be synced with a verified source like NPL clock, ISRO clock, etc. to prevent denial or service, unauthorised availing of service after due date, and unauthorised access of confidential data (e.g., viewing of bids before closing time) through tampering of server clock time. A log should be maintained for any change in server time, and such changes should also trigger SMS / E-mail alerts to designated officials.

(l) Guidelines to be prepared by the organization concerned for comprehensive audit on the lines of e-procurement 'Guidelines for compliance to Quality requirements of e-procurement Systems' issued by MeitY, also mandated by Ministry of Finance.

(m) Audit trails: All the IT systems (Hardware & Software) should maintain audit trails which can establish the digital footprints of the user login, access duration, etc. These logs must be enabled and maintained for appropriate period as per extant guidelines of the Government.

(n) Forensic readiness: E-Services should have robust forensic readiness so as to maintain usefulness of incident evidence data and ability to perform forensic investigation quickly and with ease. Organisation should have policy for recording, preserving, validating the transactions & activity logs records. E-Services should be periodically tested for their forensic readiness in case of breach or manipulation by insiders or external actors.

(o) Continuous monitoring and visibility: ICT infrastructure facilitative e-services should be continuously monitored for the security status and visibility on operations. Apart from monitoring the e-services itself, organisations should maintain ongoing awareness of information security, assets, vulnerabilities, and threats to protect the systems and prevent cyber-attacks and misuse from external as well as internal actors.

(p) Awareness: Operators, insiders and owners of the e-services could intentionally or unintentionally facilitate breach or manipulation of the e-services. A role-based information security awareness program including concepts of external and internal threats needs to be devised for key staff members. The awareness program may also include vendors and suppliers of the e-services. Senior management may monitor effectiveness of such programs.

(q) Capacity Building: Regular training programs encapsulating the major areas of vulnerability, system and security audit, robustness of IT infrastructure, etc. should be organized for the key managerial, IT personnel and other staff members of the concerned public organizations.

(r) In case, the deployed software and hardware are not security audited, it should be done at the earliest by STQC or CERT-In empanelled agencies. These audit certificates, if displayed on the home page of the IT system, will instil a sense of confidence in the minds of the users.

(s) When a software system is developed through a hired agency, ample care should be taken to distinguish the software developed and testing setup from the life setup. This means that the server or machine used for development and testing must be different from the server or hardware where software is going to be operated preferably at a different place.

(t) All the IT systems in operation must ensure periodic re-audit every two to three years or when a major functional change has been incorporated.

(u) IT systems must use digital signature system, e-sign, OTP or biometric based user authentication rather than just relying on user ID and password. Additionally, the system of screen logs out after an appropriate time lapse as may be decided by the organisation can also be introduced so as to ensure safeguard against any unauthorised person's access to the system. Besides, sensitive documents should be encrypted before transmission. For example - in an e-tender system a technical bid as well as financial bid should be encrypted so that nothing is visible to the back-end staff.

(v) Periodical Joint Review: Chief Vigilance Officer needs to take up a periodic review to ensure integrity of the existing automated systems and processes. Such review shall be carried out at-least once a year by a Committee comprising an officer of Vigilance Department, HR Department and IT Department of the Organization. A report on such review shall be submitted within one month to the Head of the Organization. Any serious deficiencies identified during the review shall be examined from vigilance angle and further investigation taken up wherever required.

(w) Government has empanelled information auditing organisations to facilitate regular audits of ICT infrastructure. Guidelines related to good information security audit practices are published for auditees, auditors, data handling and Cyber security audit baseline requirement.

For further details the following weblinks may be visited: -
https://www.meity.gov.in/writereaddata/files/CISCO Roles Responsibilities. pdf
https://www.cert-in.org.in/PDF/guideline_auditee.pdf
https://www.cert-in.org.in/PDF/Auditor Guidelines.pdf
https://www.cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf

*****

Source: GFR and Manual for Procurement issued by Ministry of Finance, Department of Expenditure.