General Administration Department (Information Technology)

2.2 Information Technology Audit of e-Tendering System in Government Departments

Executive Summary

The Government of Maharashtra adopted the e-Tendering system in August 2010 with a view to enhancing transparency in Government procurement of goods, services and works, reduce cycle time and cost of procurement. Two e-Tendering application systems were in use in the State namely, (i) Sify-NexTenders system developed by a private agency, and (ii) National Informatics Centre (NIC) system.

An IT Audit of both the systems conducted for the period 2010-16 revealed that implementation of dual systems breached the Central Vigilance Commission guidelines for use of a common unified platform for achieving economies of scale and reducing threat to security of data. While the NIC system was free of charge to users, the Sify-NexTenders system involved user charges. There were serious system deficiencies in Sify-NexTenders system which undermined the effectiveness of the e-Tendering process. The State Government also did not ensure development and implementation of all the essential features in both the systems to ensure transparency in e-Procurement process.

There were no validation checks to ensure minimum time to be allowed to the bidders for bid submission, leading to participation of a few bidders in the e-Tendering process. Comprehensive audit of Sify-NexTenders system was not done by Standardisation Testing and Quality Certification Directorate, GoI and the State Government also failed in its role to ensure this. The monitoring of the systems was poor due to insufficiency of MIS reports. Inadequate IT security, non-documentation of IT security policy, business continuity and disaster recovery plans, and deficiencies in audit trail made the systems further vulnerable to errors and manipulations.

2.2.1 Introduction

Electronic tendering (e-Tendering) is the use of Information and Communication Technology (web based) by Government in conducting their tendering processes with suppliers for the acquisition of goods, works and services. Government of Maharashtra adopted e-Tendering for tendering process in August 2010 with the following objectives:

- to provide single window system for all Government services;
- to establish a one stop-shop providing all services related to Government procurement;
- to bring about procurement reform across the Government Departments through process standardization;
- to reduce cycle time and cost of procurement; and
- to enhance transparency in Government procurement.

As per the Government Resolution (GR) of General Administration Department issued in August 2010, all the State Government Departments were mandated to use e-Tendering system from 01 October 2010 for all tenders having an estimated value of ₹ two crore and above for procurement of goods, services and works. The estimated value of tender to be procured through e-Tendering system was reduced to ₹ 50 lakh and above from 01 December 2010, ₹ 10 lakh and above from 01 October 2012 and ₹ three lakh and above from 26 November 2014.

Two e-Tendering application systems are in use in the State namely,
(i) Sify-NexTenders system of Sify Technologies Limited: The application had web based architecture and its database was maintained in MS SQL Server[1]. The application was hosted at State Data Centre in Mumbai and was available on https://maharashtra.etenders.in.
(ii) National Informatics Centre (NIC) system: The application had web based architecture and its database was maintained in PostgreSQL Server[2]. The application was hosted at NIC Data Centre in New Delhi and was available on https://mahatenders.gov.in.
The NIC system was being used mainly by Water Resources Department, Public Health Department, Agriculture Department, Industries Energy and Labour Department, School Education and Sports Department. Whereas, Sify-NexTenders system was being used by Public Works Department, Medical Education and Drugs Department, Tribal Development Department, Home Department, Women and Child Development Department.

2.2.2 Organisational Setup

The Principal Secretary, (Information Technology) in General Administration Department (GAD), Government of Maharashtra (GoM) and the Directorate of Information Technology, GoM (DIT) in coordination with Sify Technologies Limited and NIC is implementing the e-Tendering system in the State of Maharashtra. All Government Departments/undertakings/ autonomous organisations in Maharashtra were the users of the e-Tendering system.

2.2.3 Audit Objectives

The audit objectives were to assess whether:

- the e-Tendering system was effective;
- the input, processing and output controls of the e-Tendering system were adequate to ensure integrity of the system and that it complied with the rules and procedures;
- reliable controls were in place to ensure data security and that necessary tamper-proof audit trails have been incorporated in the system; and
- the system met the requirements of internal audit.

[1] It is a relational database management system developed by Microsoft
[2] It is an open source object-relational database management system

2.2.4 Audit Criteria

The planning and implementation of the e-Tendering system, data management and monitoring were examined with the provisions contained in the following documents:

- Maharashtra State e-Governance Policy 2011;
- Manual of Office Procedure for Purchase of Stores by the Government Departments issued by Industries, Energy and Labour Department in October 2015;
- GRs and circulars issued by GAD and DIT and Request for Proposal (RfP) issued in December 2009 by DIT to select system integrator for the e-Tendering project;
- Guidelines for operational model for implementation of Mission Mode Projects by the line Ministries/State Departments under the National e-Governance Plan issued by Ministry of Communications and Information Technology, GoI in May 2006;
- Guidelines for compliance to quality requirements of e-Procurement Systems issued in August 2011 by Standardisation Testing and Quality Certification Directorate, Ministry of Communications and Information Technology, GoI; and
- Guidelines of Chief Vigilance Commissioner on e-Tendering solutions issued in September 2009.

2.2.5 Audit Scope and Methodology

Audit test-checked the records in the offices of Principal Secretary (IT), GAD, DIT and 17 units under 13 Government Departments **(Appendix 2.2.1)** implementing the e-Tendering system. The selection of Departments and the units within the Departments was done based on maximum number of tenders released during 2010-16. Data in the e-Tendering system for the period 2010-16 was analysed with the help of Computer Aided Audit Techniques in addition to manual records related to e-Procurement maintained in these units. The audit objectives, audit criteria and scope of audit were discussed with the Principal Secretary (IT), GAD in an entry conference held on 15 June 2016. The Information Technology Department, GoM (Department) was requested to have an exit conference to discuss the audit findings however, no response was received from the Department. The draft IT report was issued to the State Government in October 2016; their reply was awaited as of January 2017.

2.2.6 Audit Findings

2.2.6.1 Implementation of Dual System of e-Tendering System

The Department entered (March 2010) into an agreement with Sify Technologies Limited for development and implementation of an application software for e-Tendering, procurement of server side hardware infrastructure and its maintenance *etc.* on Public Private Partnership basis under built, own, operate and transfer model. The e-Tendering application (Sify-NexTenders) was to be

transferred to DIT free of cost at the end of five years from the Go-Live of the application or on termination of contract whichever was earlier. The e-Tendering application went live from August 2010. A service fee of ₹ 882 plus service tax was payable by the bidders per bid to Sify Technologies Limited. Scrutiny of records of DIT revealed the following:

- The Department entered (March 2010) into an agreement with Sify Technologies Limited for development and implementation of application software for a period of five years up to August 2015[3], despite being aware of the fact that GoI under the National e-Governance plan (NeGP) had declared (May 2006) e-Procurement as a Mission Mode project to create a national initiative for implementing procurement reforms. Though the Department adopted e-Tendering application developed by NIC[4] in July 2012 under the NeGP but, in the absence of an exit clause, the Department could not foreclose the contract with Sify Technologies Limited and switch over to the single system of NIC from July 2012.
- Implementation of two systems simultaneously also breached the Central Vigilance Commission guidelines of September 2009 stipulating the use of common unified platform by all Departments across a State for achieving economies of scale and reducing threat to security of data.
- While the bidders had to pay a service fee ₹ 882 per bid plus service tax for using Sify-NexTenders system, the NIC system could be used free of cost by the bidders. Further, application of uniform service fee of ₹ 882 across all tenders irrespective of their money value was another drawback in the Sify-NexTenders system.
- As mentioned in **paragraph 2.2.1**, the State Government progressively brought down the value of tenders which increased the volumes and the revenue of Sify Technologies Limited. However, the benefit of volumes was not passed on to the bidders in the form of reduction in the service fee being recovered by Sify Technologies Limited.

Recommendation 1: Considering the benefits of the use of common unified platform, the State Government may consider implementation of NIC system, which is tried and tested and also free of cost, in all the Departments across the State.

2.2.6.2 Undue Benefit to Sify Technologies Limited

Though the agreement with Sify Technologies Limited expired in August 2015 yet 216 units under Public Works Department, Medical Education and Drugs Department, Tribal Development Department *etc.* continued to use Sify-NexTenders system while 2,307 units under Rural Development Department, Agriculture Department, Housing Department *etc.* continued to use NIC system in the State as of March 2016.

In March 2016, DIT extended the post Go-Live support of Sify-NexTenders system till August 2016 and also reduced the service fee payable by the bidders from

[3] Five years from Go-Live which was achieved in August 2010

[4] No fee was payable by the users for using the application software developed by NIC

₹ 882 per bid to ₹ 300 per bid from 01 April 2016, on the ground that the e-Tendering system was functional for five years. However, DIT failed to enforce its order of March 2016 as Sify Technologies Limited continued to charge a service fee of ₹ 882 per bid plus taxes, resulting in undue benefit to the service provider.

2.2.6.3 Non-execution of Service Level Agreements with Sify Technologies Limited

As per Section 6.2 of RfP issued by DIT in December 2009, the successful bidder was required to comply with seven[5] Service Level Agreement (SLA) for ensuring adherence to project timelines, quality and availability of services. However, the Department did not execute any SLA with Sify Technologies Limited till March 2016. In the absence of SLA, the methodology and periodicity to ensure correctness of the software application free from errors/bugs, methodology of logging complaints/query of the implementing units and their resolution *etc.* could not be defined and addressed. It also pointed to deficient monitoring of various services by DIT.

2.2.7 Inadequate Documentation

Documentation of an IT system such as (i) System Requirement Specifications (SRS) addressing functional and non-functional requirements including standards and policies, (ii) System Design Documentation (SDD) including software architecture design, logical, physical database design and data dictionary, programming logic, and workflows, and (iii) user manuals relating to systems administration, installation, operation and maintenance *etc.* are necessary for a quality system and future maintenance.

Audit observed that though the agreement with Sify Technologies Limited required the technical documentation and the software source code with detailed documentation to be delivered by the service provider, the same was not delivered to DIT. Similarly, for the NIC system, except for the data dictionary, vital documents such as, SRS, SDD and manuals relating to system administration, installation, operation and maintenance were not available with DIT.

Due to absence of proper technical documentation for various stages of the system development, the extent to which the user requirements were incorporated in the system could not be ascertained. Absence of technical documentation for an important e-Governance project such as this, which has maximum public use, would not only increase the dependence on outside agency such as Sify Technologies Limited but also pose a major risk for future maintenance of the system and its up-gradation.

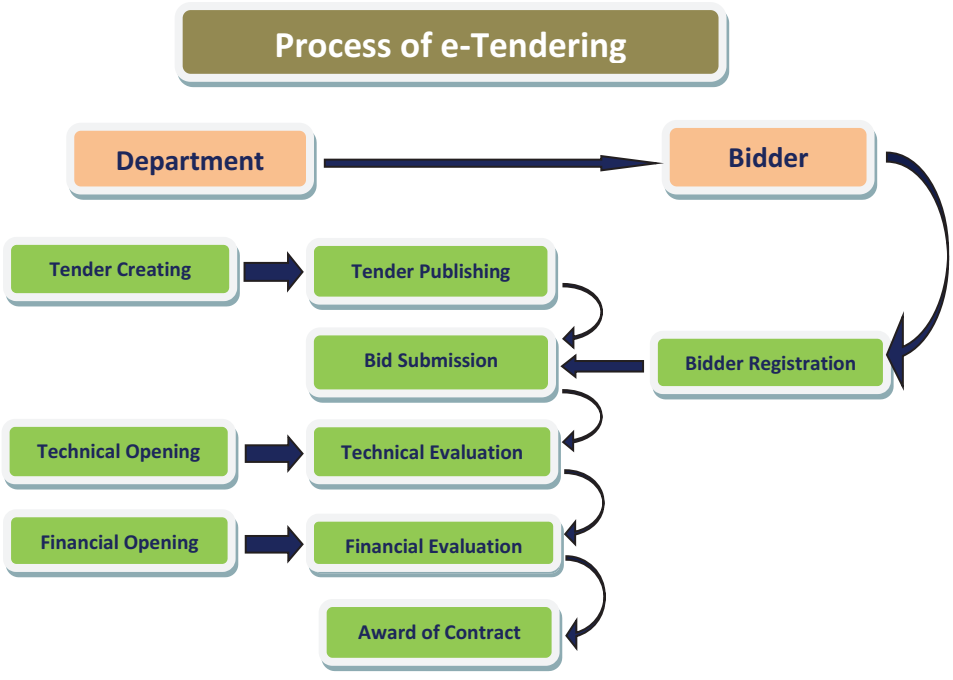
2.2.8 System Deficiencies

Functions in the e-Tendering system include online registration of bidders, tender creation and publishing, payment of tender fees and earnest money deposit (EMD), encryption of bids, bid submission, tender opening, automatic evaluation of

[5] (i) Timely delivery, (ii) Correctness of delivery, (iii) Resolution time, (iv) Installation of hardware equipment, (v) Application response time, (vi) Application availability and (vii) Security and incident management

financial bids and award of contracts. A flow chart showing the process of e-Tendering is depicted in **Chart 1.**

Chart 1



The system deficiencies noticed in Sify-NexTenders and NIC systems are discussed below**.**

2.2.8.1 Multiple Registration of Vendors

Both the e-Procurement systems provided for one-time centralised online registration of vendors before their participation in tender process. The systems captured details of vendor such as, address, nature of business, financial information, PAN *etc.* During registration, each vendor was given a unique user identity number (Id).

Audit observed that Sify-NexTenders system lacked adequate validation checks resulting in allotment of more than one user Id to a single vendor. Though, in the NIC system user Ids were validated based on e-Mail Ids, the vendors created multiple user Ids using different e-mail Ids. Both the systems did not check the registration with unique identity of the vendor like PAN to prevent multiple registrations by a single vendor. Few cases of multiple registration of a single vendor noticed in test-checked units are discussed below.

- In Directorate of Vocational Education and Training, Mumbai, 10 individual vendors were allotted more than one user Id.
- In Directorate of Government Printing and Stationery, Mumbai, seven individual vendors were allotted more than one user Id.

Thus, the information on vendors available in Sify-NexTenders system was not fully reliable as the system did not have adequate validation. In the NIC system, validation was based on e-mail Id which was not foolproof.

2.2.8.2 Inadequate Controls to Ensure Sufficient Time for Bid Submission

As per Manual of Office Procedure for Purchase of Stores by the Government Departments issued (October 2015) by Industries, Energy and Labour Department, a minimum period of one week should be allowed for submission of bids from the date of issue of tender notice in respect of procurement of goods.

However, due to non-stipulation of the minimum period for bid submission in both the Systems, the time given for submission of bids was insufficient, as discussed below.

- In the office of the Executive Engineer, Electrical Division (South), Mumbai using Sify-NexTenders system, 17 works[6] for which tender notices were issued during 2015-16, the bid submission duration was only 15 to 34 minutes (against the minimum period of one week) and the start time for submission of bid was after 10 pm. Though three to eight bidders had purchased the tenders, only one to three bidders finally submitted the bids within the stipulated time.

  The Executive Engineer, PWD (E) stated (July 2016) that sufficient time was given for all stages of tendering and that there were no irregularities. The reply is not tenable as only 15 to 34 minutes was given for bid submission stage as revealed from the data captured in the system and the time given was insufficient with reference to Manual provisions.

- In Directorate of Vocational Education and Training, the bid submission duration was three hours in 34 tenders[7] issued during 2013-14 (Sify-NexTenders system).

- In District Superintendent Agriculture Officer, Ahmednagar, the bid submission duration was one day in seven tenders[8] of which, in six tenders only one bidder submitted the bid while in one tender only two bidders participated (NIC system).

  The District Superintendent Agriculture Officer, Ahmednagar stated (July 2016) that due to some problem in the digital signature token system sufficient time could not be given to the bidders for submission of bids.

- In Directorate of Health Services, Mumbai, the bid submission duration was three hours in one tender[9] issued in September 2013 for purchase of iron and folic acid tablets (Sify-NexTenders system).

Inadequate time and odd hours specified for bid submission indicated absence of fair play and transparency in the e-Procurement process thus, defeating the objective of competitive bidding.

Recommendation 2: The State Government may ensure proper validation checks in both the systems so that sufficient time is available to the bidders for critical stages and the tendering process is not vitiated.

---

6 Total value of tenders: ₹ 2.84 crore
7 Total value of tenders: ₹ 14.48 crore
8 Total value of tenders: ₹ 0.71 crore
9 Total value of tenders: ₹ 7.24 crore

2.2.8.3 Technical Evaluation of Bidders not Uploaded in Sify-NexTenders System

Uploading of comparative statements of technical evaluations enhances transparency in the procurement process and enable all the stakeholders *i.e.* bidders, citizens, auditors *etc.* to access the information easily. Audit observed that Sify-NexTenders system did not have the facility for uploading the comparative statements of technical evaluations done manually by user Departments, though it was available in NIC system.

2.2.8.4 Absence of Facility for Displaying Data on Award of Contracts

As per RfP issued by DIT in December 2009, the e-Tendering system should have had a facility for issue of tender acceptance notice/letter of intent online to the successful bidder. Facility should also have been available for successful suppliers/contractors to respond to the tender acceptance notice/letter of intent using the digital signature.

Audit observed that these facilities were not available in Sify-NexTenders system nor was it ensured by DIT. Therefore, the details of vendors to whom contracts were awarded were not available in the system. In 14 of 17 test-checked units implementing Sify-NexTenders, the status of 6,743 of 7,020 tenders (96 *per cent*) released during 2010-16 was not available in the system. The remaining 277 tenders were cancelled.

In NIC system, though the facility for uploading the details of award of contract was available, the status of tenders released during 2013-16 was not updated in respect of 404 of 758 tenders (53 *per cent*) in five test-checked units[10]. The system did not have facility for raising alerts to enable the head of the unit to monitor the contracts where status of the tenders was not updated.

Scrutiny of records further revealed that in 24 tenders valuing ₹ 34.63 crore released during 2011-15 by four units[11], the works were awarded to bidders other than the lowest (L_1) while in two units[12] during 2013-16, though three tenders were released, the works were finally awarded to contractors who did not participate in the e-Tendering process.

Complete details of successful bidders in the systems would have facilitated comparison of system-generated first lowest bidder (L_1) with the bidder to whom the work was actually awarded and reporting through periodical management information system (MIS) to the competent authorities.

---

[10] (i) District Superintendent of Agriculture Officer, Ahmednagar, (ii) Directorate of Health Services, Mumbai, (iii) Joint Director of Industries, Pune, (iv) Directorate of Sports and Youth Services, Pune, and (v) Collector, Yavatmal

[11] (i) Commissioner, Women and Child Development Department, Pune: ₹ 24.90 crore (one tender); (ii) Directorate of Vocational Education and Training, Mumbai: ₹ 7.35 crore (two tenders); (iii) District Superintendent Agriculture Officer, Ahmednagar: ₹ 2.14 crore (20 tenders); and (iv) Joint Director of Industries, Pune : ₹ 24 lakh (one tender)

[12] Directorate of Medical Education and Research, Mumbai: ₹ 2.02 crore (one tender) and Directorate of Government Printing and Stationery, Mumbai: ₹ 16.40 lakh (one tender)

Recommendation 3: The State Government may ensure development and implementation of all the essential features in both the systems to ensure transparency in e-Procurement process.

2.2.8.5 Purchases made Outside e-Tendering not Mapped to the Systems

Paragraph 4.1 of the Manual of Office Procedure for Purchase of Stores by the Government Departments issued (October 2015) by Industries, Energy and Labour Department stipulated that information regarding all public goods procured by the Government Departments outside e-Tendering should be available in the e-Tendering portal.

Audit observed that DIT did not map the procedure prescribed in the Manual to the systems. Consequently, details of all purchases made by the user Departments outside e-Tendering were not available in e-Tendering portal of DIT. Test-check of tender files in two of 17 units revealed that four purchase/work orders amounting to ₹ 3.53 crore[13] were placed between November 2015 and March 2016 without resorting to e-Tendering but, these were not recorded in the e-Tendering portal. Further, even though the State Government had formulated a policy for procurement of public goods made outside e-Tendering, it was yet to come out with a policy on recording information on tenders finalised for procurement of public works and services made outside e-Tendering.

2.2.8.6 Absence of Facility for Blacklisting of Suppliers in Sify-NexTenders System

The RfP issued by DIT in December 2009 stipulated that the system intended to be procured should allow the user Departments to cancel the registration of any particular contractor or to blacklist any contractor or supplier so as to ensure that such supplier/contractor does not conduct further business with GoM. The same was also emphasised in the Manual of Office Procedure for Purchase of Stores by the Government Departments issued (October 2015) by Industries, Energy and Labour Department.

Audit observed that neither the facility for blacklisting of contractors/suppliers was available in the Sify-NexTenders system nor did DIT direct Sify Technologies Limited to provide the same. Absence of such facility may lead to the risk of participation of blacklisted/banned contractors in the tendering process.

2.2.8.7 Inadequate Management Information System

The e-Tendering system was expected to provide various MIS reports to serve as a tool for eliciting crucial information for decision-making and monitoring. Audit observed that in the absence of SRS in both the systems, the requirement of MIS was not documented by the service providers (Sify Technologies Limited and NIC).

[13] District Superintendent Agriculture Officer, Ahmednagar ₹ 3.24 crore, and Project Officer, (Integrated Tribal Development Project), Dahanu: ₹ 0.29 crore

Though both the systems contained modules for generation of MIS regarding tenders published, tenders opened, tenders cancelled *etc.*, the following vital MIS reports were not available in the systems:

- MIS on the tenders invited but not finalised for significantly long period (Sify-NexTenders system).
- MIS on tender fees and EMD collected through online system to facilitate its reconciliation with the amount remitted to Government account (Sify-NexTenders system).
- MIS on works awarded other than L_1 (Sify-NexTenders and NIC systems).
- MIS on EMD not refunded to unsuccessful bidders (Sify-NexTenders and NIC systems).
- MIS reports for audit trail to track the users responsible for transactions and the history of transactions were not available (NIC system).

In the absence of these vital MIS, effective functioning of the e-Tendering system could not be ensured.

Recommendation 4: The State Government may ensure that all the business rules related to procurement is incorporated in both the systems and also identify MIS reports for various user groups for effective decision-making and monitoring of procurement.

2.2.9 Deficiencies in Implementation of Systems

2.2.9.1 Uploading of Financial Bids in Portable Document Format

The facility to upload financial bids in template format or portable document format (PDF) was available in Sify-NexTenders and NIC systems. The financial bids submitted only in template format could be evaluated automatically by the systems and comparative statements generated.

Audit observed that financial bids were allowed to be uploaded in PDF (instead of template format) by the user Departments in 223 tenders issued during 2013-16 in two[14] of 17 units. As a result, the systems could not evaluate and generate the comparative statements automatically. The comparative statements therefore, had to be prepared manually thus, defeating the objective of automatic evaluation of financial bids.

The Executive Engineer, Mechanical Stores Division, Dapodi, Pune accepted (June 2016) the fact and stated that training for template preparation was not received by the Departmental staff from service providers.

2.2.9.2 Stipulation of Physical Submission of Bid Documents

Under the e-Tendering system, tenders with all supporting documents were required to be uploaded online by the bidders. Such a system ensured secrecy of tenders till the bids were opened.

[14] Mechanical Stores Division, Dapodi, Pune and Project Officer, Integrated Tribal Development Project, Dahanu

Audit observed that in 80 tenders released during 2013-16 by Joint Director of Industries, Pune, tenders along with supporting documents were allowed to be submitted both in electronic and physical forms thus, failing to protect the secrecy of the tenders before opening of bids. The Joint Director of Industries, Pune stated (June 2016) that proper care would be taken in future.

2.2.10 Post-implementation Inadequacies

2.2.10.1 Comprehensive Audit of Sify-NexTenders System not Conducted

According to guidelines for operational model for implementation of Mission Mode Projects by the line Ministries/State Departments under the NeGP issued (May 2006) and guidelines for compliance to quality requirements of e-Procurement systems issued (August 2011) by Ministry of Communications and Information Technology, GoI, the e-Tendering applications should be comprehensively tested/audited and approved by Standardisation Testing and Quality Certification Directorate, GoI (STQC) or any other Government organisations providing quality certifications. The comprehensive audit *inter alia* entailed coverage of (i) testing of application software to validate that the application met the functional requirements, and (ii) application security testing to unearth various applications security vulnerabilities, weaknesses and concerns related to the system.

Audit observed that the NIC system was audited and certified (February 2015) by STQC which was valid up to 17 February 2016[15]. However, the Sify-NexTenders system was audited (October 2013) by STQC only for application security and not for functional requirements. Consequently the Sify-NexTenders system remained incomplete as discussed in **paragraph 2.2.8.4**.

2.2.10.2 Capacity Building and Training

As per paragraph 13 of Maharashtra State e-Governance Policy 2011, the State Government would endeavour to build capacities within the system for e-Governance, program and change management by training the manpower and deploying appropriate infrastructure and machinery. The implementation guidelines issued (July 2011) by Ministry of Communications and Information Technology, GoI for e-Procurement rollout in States under NeGP further stipulated initial and continuous training and handholding support to identified Departmental staff at a defined minimum level through Facility Management Personnel (FMP). Accordingly, 30 personnel were hired by DIT in July 2012 through a private agency for various posts such as, Project Manager, Operations Manager and Operations Assistant to assist, train and support the Departmental staff using NIC system. This arrangement was however, discontinued after January 2016.

Three test-checked units[16] using NIC system confirmed to audit between April and June 2016 that sufficient training had not been provided by FMP. Further, the

[15] Re-certification is required only if major changes in the e-procurement application software are effected

[16] Directorate of Sports and Youth Services, Pune; Joint Director of Industries, Pune and Collector Office, Yavatmal

District Superintendent Agriculture Officer, Ahmednagar hired a consultant for operating the NIC system during 2014-15 and incurred an expenditure of ₹ 9.45 lakh, due to non-availability of trained manpower. These clearly indicated that DIT and user Departments did not make adequate efforts for capacity building in order to ensure seamless implementation of e-Tendering system.

Recommendation 5: The State Government may take necessary steps to build capacities within the Departments to facilitate smooth implementation of e-Tendering system in the State.

2.2.11 Information System Security

2.2.11.1 Absence of Information Technology Security Policy

An effective IT security policy is important for protection of information assets created and maintained by IT and IT enabled activities. By enunciating an IT security policy, the organisation demonstrates its ability to reasonably protect all business critical information and related information processing assets from loss, damage or abuse and also creates enhanced trust and confidence between organisations, trading partners and external agencies as well as within the organisation. Audit however, observed that the Department did not frame IT security policy nor did it issue any security guidelines and access control policies for e-Tendering system.

2.2.11.2 Non-conduct of Third Party Security Audit

As per Central Vigilance Commission guidelines of September 2009, the IT application should be audited for complete security of the system and transaction data by a competent authority at least once in a year.

Audit observed that the security audit of Sify-NexTenders system was conducted only up to October 2013 as per 'OWASP[17]-Top 10 web application vulnerabilities for 2010' while for NIC System, the application security certificate indicated that the security audit was conducted only up to February 2014 as per 'OWASP-Top 10 web application vulnerabilities for 2007'. Now that 'OWASP-Top 10 web application vulnerabilities for 2013' had been released and in use, the additional vulnerabilities such as, sensitive data exposure, missing function level access control, using known vulnerable component not initially covered in 'OWASP-Top 10 web application vulnerabilities for 2007 and 2010' remained undetected for corrective action.

2.2.11.3 Inadequate Logical Access Controls

In the computerised system, access to data need to be restricted to authorised individual users only. Audit observed that logical access controls available in both the applications were inadequate due to following reasons:

17 OWASP or Open Web Application Security Project aims to educate developers, designers, architects, managers and organisations on the consequences of the most important web application security weaknesses. As per guidelines issued in August 2011 by STQC Directorate, Ministry of Communications and Information Technology, GoI, OWASP guidelines were to be used for security testing

- In PWD Electrical Division (South), Mumbai using Sify-NexTenders system, 64 tenders valuing ₹ 26.64 crore which were beyond the financial bid opening powers of the Executive Engineer were opened (2015-16) using the user ID of Executive Engineer. This indicated that access controls for various levels of users of the system were not mapped as per the business rule.
- In PWD Electrical Division (South), Mumbai, an unknown user Id '*myshankpale_am'* was created in the system and details incorporated in 25 tenders[18] were tampered with by using this unknown user Id due to which, these tenders had to be cancelled subsequently and fresh tenders had to be invited[19]. The serious security breache was not communicated to DIT by the user Department and Sify Technologies Limited for further investigation and remedial action. The PWD Electrical Division (South), Mumbai confirmed (July 2016) that user Id '*myshankpale_am'* was not an authorised user.
- While accessing the application, a notification that 'the user is using Government Information System and its usage may be monitored' was not displayed on the website in both the systems. The date and time of the last login and the number of unsuccessful attempts since the last login was not notified in both the systems as required under eSAFE-GD220 guidelines issued (January 2010) by Ministry of Communications and Information Technology, GoI for assessment of effectiveness of security controls.
- 'CAPTCHA', a computer programme to determine whether or not the user is human, was not in use in both the systems as required under eSAFE-GD220 guidelines.
- As per the eSAFE-GD210 guidelines issued (January 2010) by Ministry of Communications and Information Technology, GoI for implementation of security controls, a computerised system should enforce change in password after a specified period (typically 30 days). This was not enforced in both the systems. In Directorate of Medical Education and Research (DMER), Mumbai, digital signatures of two officials, already transferred from the office in January 2016, continued to be used (July 2016) for opening of financial bids.
- In DMER, Mumbai using Sify-NexTenders system, user Ids were created for generic users such as *'DIR_DMER_OP'* and *'DIR_DMER_AU'* due to which, the name of officials actually using the system could not be ascertained.

Thus, the logical access controls were weak in both the systems and DIT as well as the user Departments did not sensitise the information security risks to the users of the system.

2.2.11.4 Digital Signature not Validated

Under the Information Technology Act, 2000, holder of a digital signature, whose digital signature certificate (DSC) has been issued by a licensed

[18] Tender Notice No. 9 of 2015-16
[19] Tender Notice No. 12 of 2015-16

certifying authority (CA), was responsible for protecting the corresponding private key. Unless the validity of DSC had expired or the certificate had been revoked by the issuing CA, the digital signature would be legally valid and would be attributed to the person listed in the DSC.

Audit observed that in Sify-NexTenders System, there was no provision for online verification of validity of DSC while in the NIC system, this provision was available.

2.2.11.5 Lack of Business Continuity and Disaster Recovery Plan

An organisation should have a business continuity and disaster recovery plan with associated controls in order to ensure that it accomplishes its mission and not lose the capability to process, retrieve and protect information in case of eventualities due to interruption or disaster leading to temporary or permanent loss of computer facilities and data.

Audit observed that though e-Tendering was a critical system and used throughout the State, business continuity and disaster recovery plans were not documented. Further, Sify-NexTenders system did not have disaster recovery setup and backup was taken on external storage devices, which were stored in same location as data servers. As for NIC system, the application was hosted at New Delhi and had a disaster recovery centre at Pune.

2.2.11.6 Change Management of Application not Documented

The changes to information system including its components, upgrades and modifications to the information system should be authorised, documented and controlled through the defined change management process.

Audit observed that a documented procedure for change management was not available in Sify-NexTenders system. Also, the version of the application in use was not displayed in Sify-NexTenders system for ensuring version control, as displayed on the NIC system.

Recommendation 6: The State Government may ensure documentation and implementation of IT security policy, business continuity and disaster recovery plan to protect the applications and information assets against improper or unauthorised access which could compromise confidentiality, integrity and availability of data and IT resources.

2.2.12 Inadequate Audit Trail

Audit trail captures the flow of transactions in a system in order to track the history of transactions, system failures, erroneous transactions, changes/modifications in data *etc.*

Audit observed that in Sify-NexTenders system, published tenders were selectively deleted from the live database and moved to archived database by Sify Technologies Limited for which, no audit trail existed. In the NIC system, data of previous years has been retained in the production system.

2.2.13 Absence of Audit Module

The audited entities are required to ensure that all requirements for the purpose of facilitation of audit are incorporated in the IT system and that audit has the right to access the IT systems, irrespective of the fact that the systems are owned, maintained and operated by the audited entities or by any other agency on behalf of the audited entities. Further, internal audit system both in manual and computerised environment ensures that the controls are in place.

Audit observed that there was no audit module in both the systems to generate customised reports for facilitating conduct of internal audit. Though the Sify-NexTenders system was being implemented since 2010-11, the internal audit wing did not verify the transactions through the system.

2.2.14 Conclusion

An Information Technology audit of e-Tendering system revealed that the State Government was implementing dual systems simultaneously – one through a private agency (Sify-NexTenders) and the other through NIC, in contravention of Central Vigilance Commission guidelines for use of a common unified platform. While the NIC system was free of charge to users, the Sify-NexTenders system involved user charges. There were serious system deficiencies in Sify-NexTenders system which undermined the effectiveness of the e-Tendering process. The State Government also did not ensure development and implementation of all the essential features in both the systems to ensure transparency in e-Procurement process.

There were no validation checks to ensure minimum time to be allowed to the bidders for bid submission, leading to participation of a few bidders in the e-Tendering process. Comprehensive audit of Sify-NexTenders system was not done by Standardisation Testing and Quality Certification Directorate, GoI and the State Government also failed in its role to ensure this. The monitoring of the systems was poor due to insufficiency of MIS reports. Inadequate IT security, non-documentation of IT security policy, business continuity and disaster recovery plans, and deficiencies in audit trail made the systems further vulnerable to errors and manipulations.