

## INFORMATION TECHNOLOGY AND COMMUNICATION DEPARTMENT

### 3.2 Information Technology Audit of eSeva – an e-Governance initiative by Government

#### Highlights

*Though Government launched a unique and conceptually a good project to put e-governance into action to provide a large number of services to citizens on one-stop-shop basis, the project suffered from lack of transparency, inefficient and ineffective implementation largely due to unpreparedness of the participating departments and inadequate coordination. The network was exposed to serious risks of physical access controls and logical controls. The key data and huge volumes of cash pertaining to various departments had been left to the administration of private operator without adequate internal controls. Data integrity, reliability, and safety across the project were also inadequate.*

❖ The eSeva project, a New Service, was started without formal budget provision and without conducting feasibility study. Financial rules were largely neglected by the Director, eSeva project in implementing the programme. The project was rushed through even when the participating departments were not ready.

*[Paragraphs 3.2.4 (i) and 3.2.6]*

❖ The bid evaluation adopted in selecting the operator lacked transparency, and only one operator was selected instead of two in violation of the Government orders.

*[Paragraph 3.2.4 (ii) and (iii)]*

❖ Adequate documentation did not exist for any of the aspects relating to software, hardware, network, error handling, etc. Complete technical documentation including the source code specified in the tender was also not obtained. This had resulted in a situation where the Director was completely dependent on the operator. Adequate business continuity plan also did not exist.

*[Paragraph 3.2.5 (ii) and (iii)]*

❖ The essential controls in computerised environment such as logical access controls, physical access controls, etc. were found inadequate. The network security of the project was also lacking.

*[Paragraph 3.2.5A (i) and (iii)]*

---

The abbreviations used in this review are listed alphabetically in glossary vide Appendix XXXVI (page 212)

❖ **The transactions in eSeva were not reconciled with the data in the respective departments and scrutiny revealed many irregularities, inadequacies and inconsistencies in the data.**

[Paragraph 3.2.5A (iv)]

❖ **Government assets worth Rs 90 lakh relating to the TWINS pilot project were handed over to the operator free of cost though not provided in the agreement.**

[Paragraph 3.2.7 (iv)]

### 3.2.1 Introduction

Government implemented (December 1999) a unique pilot project “Twin Cities Network System” (TWINS) (cost: Rs 90 lakh) as part of e-governance to provide speedy services across the counter integrating several departments<sup>27</sup> and Public Sector Undertakings/ Local Bodies<sup>28</sup> in an efficient, reliable and transparent manner, computerised under one-stop shop arrangement to citizens in a limited jurisdiction. Government decided (June 2000) to extend the TWINS project to twin cities of Hyderabad and Secunderabad by opening a chain of 24 integrated citizen service centres and renamed the project as eSeva. The project was to be implemented on Build Own Operate and Transfer (BOOT) basis under Public-Private Partnership model where Government would provide civil infrastructure and private operator would provide IT infrastructure including Hardware, Design and Development of Software. The role of participating departments was limited only to allowing access to eSeva authorities, their database and to permit them to update the same on the basis of day to day financial transactions carried out in the various eSeva centres.

The eSeva project was designed on a 3-tier architecture. The first tier consists of counter terminals and printers located at eSeva centres and the second tier consists of web servers and firewall servers located at Data centre (Khairatabad). The third tier consists of departmental servers located at different departmental offices, the services of which were offered at eSeva centres. All systems were connected in a network with leased lines and ISDN<sup>29</sup> backup.

### 3.2.2 Salient features

The salient features of eSeva project *inter alia* are to (i) provide real time online transaction; (ii) provide various services like payment of electricity and telephone bills, booking of

---

<sup>27</sup> Registration and Stamps, Transport, Commercial Taxes, Ministry of External Affairs, etc.

<sup>28</sup> Bharat Sanchar Nigam Limited, Transmission Corporation of Andhra Pradesh Limited (APTRANSCO), Hyderabad Metropolitan Water Supply and Sewerage Board (HMWS&SB), Municipal Corporation of Hyderabad (MCH)

<sup>29</sup> Integrated Services Digital Network

bus tickets, obtaining birth certificates, filing tax returns, etc., at any counter and at any centre; (iii) provide IT infrastructure and its maintenance for a period of 5 years by the operator (contractor firm), which is to be transferred at zero value to Government after 5 years; (iv) collect revenue relating to various departments/PSUs, etc. through eSeva and (v) not to levy service charge on the citizen and the transaction charges were to be paid to the operator by Government.

The eSeva initiative is an e-Governance initiative which facilitates citizen interface with the Government and reduces the inconvenience caused to citizens in visiting multiple establishments of the Government for getting various services; resulting in time saving. While the number of daily transactions was around 600 in August 2001; the number increased to 3202 in March 2002. As of August 2002, there were 21<sup>30</sup> eSeva centres in twin cities of Hyderabad and Secunderabad and 23.78 lakh transactions involving Rs 296.57 crore were carried out in these centres.

### 3.2.3 Scope of Audit

The scope of audit included test-check of the records of the Director, eSeva for the period August 2001 to March 2002 and verification of the general and application controls operating in the IT environment. Data pertaining to the period of three months (January – March 2002) was chosen for substantial checking of data completeness, regularity and consistency, using an audit software tool namely IDEA (Interactive Data Extraction and Analysis) package. The findings of the audit are discussed in succeeding paragraphs.

### 3.2.4 Programme implementation

**Feasibility study not conducted before taking up the scheme**

The hardware items in the Project *inter alia* included web application server (SunE 250 512MB RAM 20 GB x 5 hard disk with raid 5 implementation servers), Database server (Compaq ML 530), Firewall server (IBM Netfinity 3000), web server (Compaq ML 370), two standby servers, 150 PC systems, printers etc. The application software was developed by M/s. Ram Informatics Limited and the system software/RDBMS (Relational Database Management System) used in the project for developing applications by the operator included Oracle 9iAS on solaris, Oracle 8i on Windows 2000 at Data centre (Khairatabad) and Windows 95 with internet explorer (IE5) at each of the eSeva centres.

<sup>30</sup> Bahadurpura, Banjara hills, Darulshifa, Greenlands, Khairatabad, KPHB, Habsiguda, Malakpet, Maredpally, Mint Compound, Musheerabad x Road, New Nallakunta, Ramnagar, Rethi Bowli, Sanjeeva Reddy Nagar, Santoshnagar, Seetaphalmandi, Sultan Bazar, Tirumalagiri, Vijaynagar colony and Vanasthalipuram

*i) Feasibility study of the project not taken up:* Audit scrutiny revealed that feasibility study of extending the service both technically and commercially was not conducted before implementing the TWINS expansion (eSeva) project. As a result, the suitability of the solution offered by single operator and the total resources required for the project such as staff, hardware, software, etc could not be accurately assessed by the Government.

**Evaluation of bids lacked transparency**

*ii) Lack of transparency in evaluation of bids:* (a) Based on the procedure stipulated in the bid document, the evaluation committee<sup>31</sup> short-listed (July 2000) four firms after technical bidding and invited these firms for financial bidding. After opening (October 2000) financial bids of four short-listed firms, the conditions in the Request for Proposal<sup>32</sup> (RFP) were altered (October 2000) and revised financial bids were obtained from these four short listed firms. Further, the technical scores initially assigned were revised by the evaluation Committee (only three out of 10 members<sup>33</sup> were present) assigning highest marks to the firm which got least scores in the initial evaluation. The evaluation committee did not record any reasons for changing the initially assigned technical scores. The process lacked justification and transparency.

(b) Later, the evaluation committee further short-listed two firms viz., CMS Ram Informatics (RIL) and Tata Consultancy Services (TCS) and recommended (October 2000) to conduct negotiations with both the firms. The negotiating committee adopted the lowest price quoted (slab rate: Rs 3.95 per utility transaction) by TCS as benchmark price for further negotiations. Finally after negotiations, RIL which quoted slab rate of Rs 4.75 per utility transaction<sup>34</sup> and which got least technical score in the initial evaluation process was awarded (December 2000) the contract at the benchmark price. Further, the committee allowed (November 2000) upward revision (Rs 6 to Rs 8) of the paper based transaction cost in respect of two services pertaining to reservation of ticket bookings and filing of applications / forms.

Thus adopting the lowest price quoted by TCS as benchmark price, and not asking TCS during the negotiations to further reduce its price while awarding the contract to RIL at benchmark price was irregular.

**Against the initial decision to select two private operators, all the centres were entrusted to only one operator**

*iii) Dependence on single operator:* Government initially decided (June 2000) to select two private operators for establishing eSeva centres to generate required competition and to provide choice

---

<sup>31</sup> consisting of MD/APTS (Chairman), Director, eSeva and other eight members from Transport department, APTRANSCO, Telecommunications, etc.

<sup>32</sup> RFP is in the nature of tender schedule in works contract

<sup>33</sup> signed by only two members

<sup>34</sup> Up to 3.60 lakh transactions : Rs 4.75 per transaction and, above 3.60 lakh transactions : Rs 3.95 per transaction besides different rates for different services

to citizens based on performance of respective centres. Accordingly bids were invited (June 2000) for selecting two operators for the purpose. However, all the centres were entrusted to only one operator without assigning any reasons. The objective of maintaining competitive spirit in quality of service, thereby providing choice to citizens was defeated.

**Project administered with adhoc arrangements on day to day basis**

*iv) Lack of segregation of duties:* There was no clearly defined role for each of the nine administrative personnel working in the eSeva Directorate and the project was being administered with adhoc arrangements on day to day basis exposing itself to high risk of lack of accountability. Also the entire private staff appointed by the operator working at Data Centre (Khairatabad) were having access to servers, database, application software, operating system and associated utilities exposing the system to risk of unauthorised access and data manipulation.

**SRS document not prepared at all at planning stage**

*v) Lack of System Requirement Specifications (SRS):* The system requirement specifications that ultimately guide system design work were expected to be carefully decided specifying the access controls, regulatory requirements, and operational considerations. It was important that all the participating departments/agencies and user groups be actively involved in the process of developing requirements. However, it was noticed in audit that the SRS was not at all prepared and everything was left to the discretion of operator exposing the project to serious risks of scope creep (process of changes during development and implementation).

### **3.2.5 Programme performance**

*i) Time and Cost Overrun:* The eSeva centres were scheduled to be fully operational from January 2001. However, due to delay in (i) identification of sites for locating eSeva centres, (ii) updating the data in participating departments/agencies, (iii) developing application software, (iv) procuring IT infrastructure, and (v) non-completion of civil works, the project suffered time overrun and only 17 out of 24 eSeva centres targeted were set up as of March 2002. The IT&C Department sanctioned Rs 258 lakhs in June 2000 for developing civil infrastructure required for 24 eSeva centres, as against which an expenditure of Rs 328 lakhs was incurred for developing civil infrastructure in 17 eSeva centres established as at the end of March 2002. The department neither rendered detailed account for amounts drawn, nor got the additional expenditure ratified by competent authority.

**Complete technical documentation including source code not obtained**

*ii) Lack of system documentation policy:* There being no policy regarding maintenance of essential documents with eSeva, adequate documentation did not exist for any of the aspects relating to software, hardware, network, error handling, etc. with the eSeva.

The Director did not obtain various documents specified in the tender such as the complete technical documentation including source code resulting in complete dependency on the operator. Absence of source code would make it impossible for identification of any unauthorised programme running in the software application package. The Director stated (August 2002) that the source code would be obtained from the operator at the end of contract period. This was against the terms of the agreement, according to which it was to be furnished at initial stages itself.

**Inadequate  
business  
continuity plan  
and absence of  
back up devices  
for offline  
transactions**

*iii) Lack of adequate business continuity and disaster recovery plan:* There was no documented business continuity and disaster recovery plans defining the roles, responsibilities, rules and structures for continuing the operations of eSeva in the event of any disaster caused either due to intentional, accidental or natural calamities. There were no fire fighting systems both at data centre and eSeva centres. There was no attempt to classify assets and data on the basis of any risk perception of the department. Audit further observed that:

- As against more than 17 routers used for day-to-day operations, only two back-up routers were available at Khairatabad data centre.
- No alternative site had been identified for data centre activities in case of any disaster.
- In case of offline transactions, no back-up devices were in place at eSeva centres. Adequate alternate arrangements for continuing the transactions in the absence of key personnel for any reason, were also not in place.
- The back-ups of online data taken by the operator had not been tested for recovery so far. The backup of online data was not available with any Government Officer of eSeva though the Government was the owner of the data.
- Alternate means of collecting utility payments when eSeva centres do not function for various reasons were also not in place. It was important in a scenario where eSeva centres are being developed as only collection centres for many payments with the closure of existing manual collection centres.
- Scrutiny also revealed that backup of user level exports was being taken on a daily basis without any facility of hot backups in place exposing the system to serious data safety/ recovery risks. In a project of this scale where more than 20000 transactions are taking place daily, a strong back up strategy with a judicious mix of hot and cold backups was an urgent requirement.

## A. Security management

**Entire network exposed to risk of misuse by offenders**

*i) Inadequate physical access controls:* Though stipulated in the agreement, the operator did not make sufficient security arrangements in Data centre and the eSeva centres. Physical Access Controls, which are essential to protect the eSeva centres from unauthorised access were inadequate exposing the entire network to the risk of misuse by the offenders. In one incident, there was a theft of systems and expensive devices like Router (total cost : Rs 3 lakh) at one of the centres<sup>35</sup> on 31 July 2001. This incident of theft demonstrates the security inadequacies besides exposing the entire network to the risk of misuse by unauthorized persons.

**User account management system not adequate**

*ii) Inadequate password/user account management:* (a) There was no well-defined documented password policy for the eSeva application, Oracle Database and operating system. There was no restriction on unsuccessful login attempts. The date and time of last access and number of unsuccessful attempts after last successful login attempt were not being displayed on the screens of authorised users at the time of login. There was no validation check to reject password creation of very short length. There was no system of maintaining emergency passwords, which had to be kept in a sealed cover with responsible authority for use in unforeseen situations. It was also noted that Passwords were not case sensitive.

(b) There was no documented well-defined procedure for creating user accounts. Though over 150 Data Entry Operators (DEO) access application software on any day, adequate user account management system was not in place.

**No online monitoring both at eSeva centres and Data centre – network exposed to risk of access by unauthorised users**

*iii) Lack of network security:* (a) It was observed that the Director had not conducted a review of functioning of network management tools to identify weaknesses. The difference in number of transactions as reported by eSeva and two participating organisations viz., APTRANSCO and HMWS&SB (Paragraph 3.2.5A(iv) also refers) indicate that data transmission was incomplete on some days. There had been no online monitoring both at eSeva centres and Data centre to monitor the activities of the operator/manager/programmer. Protocol analysers, essential for ensuring network security were not being used. The central server of Data Centre which is a primary installation for operation of the project, was itself located within one of the eSeva centres (Khairatabad) thereby exposing the network to risk of access by unauthorised users.

**Data transmitted in clear text instead of in encrypted form**

(b) There was no procedure to classify the data depending upon its sensitivity to protect highly sensitive data. The data was being transmitted in clear text between eSeva centres to data centre instead

<sup>35</sup> eSeva centre at Ramnagar

of in an encrypted<sup>36</sup> form. The risk of splicing the wire and re-routing the data to a private location cannot be ruled out. The Director, eSeva stated (August 2002) that encryption was not adopted as it involved additional load and would reduce system performance. The reply was not acceptable in view of the risks involved and data encryption cannot be overlooked on account of load constraints.

*iv) Irregularities in data:* Scrutiny of transactions from January to March 2002 revealed deficiencies as listed: (i) The total number of transactions as well as total amount as per reports generated in the system did not tally with the figures in reports generated by Audit using the sample data (ii) There were gaps in transaction numbers in respect of data generated at some of the eSeva centres. This indicated that the transactions were being deleted altogether. Since the programme permitted such deletion, it was a serious threat to the security of data and unauthorised deletion of transactions without trace had wider ramifications and enhanced the risk of frauds. It was replied that since there was no cancellation option in the program developed, whenever the operator posted the transactions with wrong details; those transactions would be deleted at the database level by DBA. Including a service without adequate provisions to take care of operational problems was not a good practice. Further, deleting a transaction even by DBA was a risky practice; (iii) In as many as 9277 transactions involving Rs 68.43 lakh pertaining to electricity charges to APTRANSCO the consumer's name was blank which indicates that the departmental data base was incomplete, and the project was hurried without sorting out issues relating to interface with departments; (iv) The amounts did not tally in as many as 4251 transactions, the difference of Rs 2.32 lakh remained to be reconciled. Similarly 24176 transactions covering more than Rs 18 crore recorded in the eSeva database were not recorded in the APTRANSCO database; indicating serious deficiencies in updating the TRANSCO server from intermediate server; (v) As many as 80 transactions recorded in eSeva database, were not recorded in HMWS&SB database; indicating existence of undetected bugs in programme; (vi) In 11515 transactions covering Rs 81.64 lakh the transaction numbers, which was one of the key fields for updating the HMWS&SB server were not recorded rendering it difficult to trace back the transactions when required; (vii) As per the agreement, the APSRTC would pay a commission of Rs 10 per transaction to eSeva out of which the eSeva was to pay Rs 8 to the operator. Scrutiny revealed that the total number of transactions as reported by eSeva were at variance with APSRTC database on certain dates; the amount exhibited in eSeva reports did not tally with the amounts exhibited in APSRTC

---

<sup>36</sup> Encryption is a process of converting a plain text message into a secured coded form of text for protecting data in transit over networks from unauthorised interception, manipulation, or alterations of data

**Excess amounts paid by eSeva to APSRTC**

**Receipts issued in eSeva centres not numbered and accounted for**

database. The invalidation of tickets exhibited in APSRTC database did not find place in eSeva database and excess amounts were paid by eSeva to APSRTC on certain dates; (viii) The updation of the database in the server of APTRANSCO from intermediary server installed for eSeva transactions was not being done regularly. The data posted into eSeva server was incomplete as essential details like consumer number, name and address, etc. in many cases were not available, leading to complications in collections, in former bill collection centres converted into eSeva centres. Reconciliation of payments made in eSeva centres since inception of the centres was not completed by any of the 17 Electricity Revenue Offices (EROs) as of April 2002. Since the receipts issued in the eSeva centres are not numbered and no account of receipts was maintained at eSeva the possibility of revenue leakages cannot be ruled out. The Director stated (August 2002) that network computers billing software and connectivity would be provided to overcome these problems.

v) ***Inadequacies in e-payments module*** : The eSeva envisaged providing online services through internet to citizens. As of date only payment of utility bills of TRANSCO, HMWS&SB and MCH services were provided through internet. The operator had not shared the network diagram, firewall configuration, etc. which ensure existence of proper physical and logical security with the eSeva authorities. The value of degree of reliance on the firewall and the security, probability and extent of the potential for direct and indirect harm from intruders, hackers, etc. had not been properly tested by competent technical experts. In the absence of proper documents and information, at least periodical penetration tests to ensure security of the system should have been conducted. However, no evidence of eSeva authorities getting penetration test conducted was produced to Audit. The eSeva authorities replied that the internet security aspects were reasonably tested by Price WaterHouse Coopers (PWC) before inauguration of eSeva centres. However, the PWC clearly stated that as part of Network Security review they had reviewed the operating systems on which critical applications and data base were running and CISCO Routers, and the list of modules reviewed by them did not cover the e-payments. Thus there was no evidence of PWC conducting any review of internet security aspects. Viewed in this context, it appeared that the Director eSeva was totally dependent on private operator and had no mechanism to check the correctness of claims made by the private operator. A test check of e-payment transactions revealed that the validations incorporated in the programme were inadequate. To cite a few inadequacies (i) The system was accepting less than the bill amount towards electricity charges, while the TRANSCO clearly stated that eSeva was not authorised to collect any amount other than the bill amount from consumers; (ii) The system was accepting electricity charges even without capturing essential details

of name of consumer, ERO (Electricity Revenue Office) /section etc. rendering posting of the amount so collected in individual account extremely difficult leave alone reconciliation; (iii) The system was accepting very low amounts (even less than the minimum tariff) due to which many transactions with paltry amounts ranging from Re 1 to Rs 39 were recorded making the operator entitled for transaction charges of Rs 20 per transaction though the minimum charges fixed are Rs 50 as enquired with APTRANSCO in respect of Electricity bills; (iv) The system was accepting property tax payments even without recording the essential details of locality, house number, name of the assessee, ward/circle etc. rendering their accounting extremely difficult. This also resulted in misclassifications and the consequent non-updation of demand of the consumers.

The logs of internet transactions were not maintained on a continuous basis. They were neither archived nor being reviewed before they were overwritten after 7 days. In view of the inadequacies in e-payment the project was exposed to serious risks. It was replied to Audit that the appropriate monitoring arrangements would be introduced from 1 September 2002 onwards.

**Recommendation  
of PWC  
(consultant) not  
implemented**

*vi) No adequate follow-up on the recommendations of PWC:* Though the operator was required to provide complete technical details which were considered while developing IT solution to the Director, eSeva as per the agreement, the operator did not share any information. To check the correctness of application packages, the Director outsourced (June 2001) the pre-launch testing to an international firm viz., Price WaterHouse Coopers (PWC). The firm pointed out (August 2001) that certain sensitive services that were not required were found to be running on the system, and the source routing in the router was not disabled besides host of other deficiencies. However, the project was inaugurated and implemented without attending to the deficiencies pointed out by the firm thereby exposing itself to high risks in common security across all platforms (routers, general controls etc.).

## **B. Control management**

**No record of  
changes made  
since inception  
of eSeva**

*i) Lack of change management system:* Any Information system of this scale requires a sound change management procedure covering control of the ongoing maintenance of system, standard methodology for recording and performing control changes. An appropriate level of administration should authorise changes to the programs. Although the operating staff initiate change process in order to resolve a processing problem or to enhance the operational performance of the system, the authorisation should still be obtained from eSeva authorities or any other designated officer before releasing for implementation. The operator should ideally submit

periodic updates to program or new release levels of software adopted to eSeva authorities to determine whether the changes and updates are appropriate to eSeva project. It was observed that changes to software application packages were being made without any formal authorisation by eSeva authorities. The authority competent to authorise changes in the application package had not been specified so far. No evidence of a review of changes made to the application package by the operator existed. This had exposed the system to frequent changes in the software applications, without the knowledge of department. In an e-Governance project of this type where the programmer who created the application package was also responsible for its operation, a well defined procedure to control the changes is essential to prevent potential frauds, misappropriations, misuse etc. The risks got compounded since, (i) there was no clear cut segregation of duties, (ii) the operator had not shared the source code with the department making review of source code impossible (by running appropriate source code comparison programme), (iii) the log management and documentation were found to be weak etc. The possibilities of operator's employees maliciously inserting extra codes intermittently and removing them for their personal benefit cannot be ruled out and there was no control even to detect such attempts.

*ii) Deficient control system:* (a) The software application package developed by the operator based on TWINS pilot project was fraught with many deficiencies and validation inadequacies such as accepting numbers in name field, accepting absurd dates, junk data in Bank and Branch code, accepting absurd ages; the amount field in MCH services (issue of certificates) was not appropriately programmed as the package was validating any amount for issue of certificates; alerts, messages and pop-ups in many screens were also inadequate, etc. Though some of the inadequacies pointed, were stated (August 2002) to have since been rectified, a comprehensive review of all the data elements were needed to be taken up by the department.

(b) Output controls which provide assurance that the data delivered to users would be presented, formatted and delivered in a consistent and secure manner, were inadequate and no mechanism existed to ensure that the reports generated by the system were complete and accurate. Some of the defects in the reports generated were as follows: (i) The Department-wise/day-wise collection summary report for month (DDR-36) developed was defective as the number of transactions extracted through this report varied with the number of transactions generated through other reports, to cite an example the total number of APSRTC ticket bookings reported through this DDR 36 to end of March 2002 was 724 while the actual number of transactions during the same period as reported by other DDR (DDR-5) was 772. When this was pointed out it was replied

that the report was under development. Any report, which does not reflect the correct position should not have been included in the module; (ii) The amount of collection as well as number of transactions reported in e-payment collection register (DDR-43) varied with the department wise collection summary. When the reports were generated using same database, variations in different reports indicated programming inadequacies; (iii) The time and date stamp was not being recorded on the reports generated by the system; (iv) The reports generated did not exhibit the pay mode for all transactions consistently.

**Absence of system to control and monitor activities of database administrator**

*iii) Inadequate control over database administrator:* The agreement with the operator provided that operator should appoint Database Administrators (DBA) for maintaining the database. Since the role of DBA was very crucial to the system, there was a need to monitor and control the activities of DBA, particularly when the responsibility of maintaining Government financial data was entrusted to an employee of a private operator. However, the Director, eSeva had no system to control and monitor activities of DBA. It was observed in audit that the project was exposed to high risks related to data integrity, system efficiency and effectiveness since there was (i) no clear cut segregation of duties to divide use of database tools and their custody and maintenance, (ii) no specific procedure for approving activities of DBA, and (iii) no log of activities of DBA were maintained making review of access logs impossible. Even manual logs regarding changes made to database did not exist. The Director, eSeva replied that since the eSeva did not maintain any data, control over DBA was not envisaged. In view of weaknesses in various controls and since reconciliation of transactions was not being done on regular basis, a suitable mechanism to control the activities of DBA would be essential.

No verification of the data updation into the departmental server to ensure the accuracy, completeness, consistency of the data had been conducted either by eSeva authorities or by any of the participating departments/agencies. Even the reconciliation of the transactions recorded in eSeva server with that of the departmental servers had also not been done since inception.

Scrutiny of the data made available to Audit also revealed that some of the transactions conducted through eSeva were deleted by the DBA from the log files. On being pointed out, the Director stated (August 2002) that those transactions were test transactions, posted into database prior to inauguration of e-payments. The reply was not acceptable as these deleted transactions pertained to the post inauguration period.

### C. Error management

None of the participating agencies/ departments had reconciled the amounts due and received by them

i) Scrutiny revealed that for some of the transactions, the transaction amount was recorded as zero even when the transaction had been conducted, which indicated that the system failed to record the transaction amounts. Further when the payments were made by cheque or DD or credit card, capturing the particulars of instrument were not recorded in respect of some transactions indicating that the system either failed to record details or accepted the transactions without entering the mandatory fields. The Director stated (August 2002) that the deficiency was due to system configuration problem, which would be prevented. The seriousness got further enhanced in view of the fact that none of the participating agencies/departments had reconciled the amounts due and received by them. It was observed that there was no documented error handling procedure for application software errors, system software errors and errors during operation. As per the procedure in vogue, all errors that occur during operation were rectified without the errors being recorded either manually or electronically, with no record of action taken on errors. This made it impossible to verify whether all the errors had been adequately rectified or not.

While there may be number of reasons for problems remaining outstanding for a longer period, it should not be acceptable for a problem to remain unresolved at all, which exposes the entire eSeva project to serious risks. Neither the eSeva authorities nor the operator had identified and designated personnel for addressing different types of errors the users encounter while operating the system.

ii) **Non-provision of audit trail:** The audit trail provides the capacity to trace source documents, to control totals and to identify source documents supporting the control totals. Scrutiny revealed that the data systems audit trail was not provided in eSeva thereby exposing the project to risks having implications with regard to reconstruction of processing when required. Though the Director stated (August 2002) that transaction logs were maintained in place of audit trail, this did not serve the purpose to trace the flow of transactions as also the processing at every stage.

iii) **Inadequate control over offline transactions:** The eSeva provides online updation of water works transactions. The transactions in case of APTRANSCO and BSNL were updated into the departmental server through batch processing at the end of the day by the department concerned. When the connectivity goes off, the transactions were entered offline to avoid inconvenience to citizens which would be processed and posted later into intermediate server when the connectivity was restored. There was a possibility that these offline transactions are deleted before these are updated in

the servers at data centre. It was however, observed that there was no procedure to ensure that all the offline transactions had been properly updated to backend servers. There was no record with the Director as to the details of date and time of data centre and eSeva centres going off-line and their restoration.

### 3.2.6 Financial management

**Expenditure incurred on 'New Service' without legislative sanction**

*i) Expenditure without sanction of Legislature:* The project was commenced (August 2001) even without a token provision in the budget (2001-02) for the purpose. In spite of that an amount of Rs 3.28 crore was spent on buildings (Rs 2.48 crore) and furniture, etc. (Rs 0.80 crore) to the end of March 2002 on 17 eSeva centres alone with a further undischarged liability of Rs 1.50 lakh. The Director neither rendered the detailed accounts for amounts drawn nor the expenditure was ratified by the competent authority (August 2002). The activity constituted 'New Service' as expenditure of the nature had not been incurred in the past two years and the expenditure was incurred without the approval of Legislature.

**Funds kept outside the government account in a large number of bank accounts without Government permission**

*ii) Disregard of financial rules by Director:* The Director was maintaining 20 bank accounts with the two nationalised and four scheduled/commercial banks without the permission of the Government. The Director also opened (December 1999) two separate savings bank accounts with two nationalised banks, this too without Government permission, for crediting the moneys received from the Principal Secretary, IT&C for incurring the expenditure on various items, instead of keeping the funds within government account. In addition to this the transaction charges (user charges) collected from the participating departments were also being kept outside the government account despite the specific instructions issued by Government in March 2001 to remit these moneys in a separate Personal Deposit (PD) account. As of March 2002, Rs 23.16 lakh<sup>37</sup> were collected as user charges from various departments. The Director was irregularly incurring expenditure from out of these departmental receipts for day-to-day implementation of the project utterly disregarding the financial rules. No cash book as envisaged in Rules was being maintained by the Director. The bank reconciliation statements to ensure correctness of account was also not being prepared.

---

<sup>37</sup> HMWS&SB (Rs 9.38 lakh), APTRANSCO (Rs 3.87 lakh), APSRTC (Rs 0.08 lakh), BSNL (Rs 3.24 lakh) and Regional Passport Office (Rs 6.59 lakh)

## 3.2.7 Other points of interest

**Huge advertising costs incurred by eSeva and participating departments though not contemplated**

<p><i>i) Non-fulfillment of contractual obligations by operator</i></p>	<p>(a) The operator had not fulfilled many of the obligations on his part as per the agreement such as (a) the agreed hardware items<sup>38</sup> were not provided, (b) the queue management system was installed only in 5 out of 18 centres, (c) instead of 18 fax machines, only 10 fax machines were provided, (d) water coolers were provided only in 5 out of 18 centres, (e) as against two attendants per shift, only one attendant for two shifts was provided, (f) as against 3 tonne AC to be provided at each of the eSeva centres, only 3 ACs in all (out of 18 centres) were provided, (g) as against 18 (5 KVA) generators, only 10 generators were provided, (h) as against the training of six weeks to be provided, only two weeks training was provided and refresher courses were never conducted, (i) user manuals in two languages<sup>39</sup> were not provided, and (j) the value of the assets created were not disclosed by the operator. Thus, the operator was allowed unintended benefit.</p> <p>(b) As per the agreement, the operator was to organise at his expense wide publicity through all media. However, advertising costs were incurred by eSeva (Rs 10.66 lakh) apart from the expenditure incurred by various participating departments.</p> <p>This resulted in extra financial burden on the exchequer and undue benefit to the private operator to that extent.</p>
<p><i>ii) Unintended benefit to operator</i></p>	<p>The RFP based on which bids were received clearly prescribed (July 2000) that the cash collection centres or other service centres of respective participating departments would continue to function even after establishment of eSeva centres. It was further mentioned that the departments would be free to establish some service centres or departmental collection centres and the Director, eSeva would not guarantee the minimum number of transactions at eSeva. These conditions were, however, not incorporated in the agreement with the operator. However, based on the request made by the operator, existing cash collection centres of APTRANSCO and many cash collection centres of HMWS&amp;SB, were closed thereby conferring undue advantage to the operator besides causing inconvenience to citizens.</p>

<sup>38</sup> Systems, LaserJet printers, Dot-matrix printers, etc.

<sup>39</sup> Telugu and English

<p><b>Extra payment of Rs 0.72 lakh to the operator on MCH services</b></p>	<p><i>(iii) MCH services</i></p>	<p>Scrutiny revealed that the solution offered by operator for issue of birth and death certificates does not provide facility of issue of certificates online. Though online certificates are not issued, the operator was being paid as per rates for providing online services i.e. transaction charges at Rs 8 per certificate in addition to Rs 3 per additional copy unauthorisedly. This resulted in avoidable extra burden of Rs 0.72 lakh in respect of 9000 transactions conducted to the end of March 2002.</p>
<p><b>Government assets worth Rs 90 lakh handed over to the operator free of cost</b></p>	<p><i>iv) Handing over of government assets to operator free of cost</i></p>	<p>The TWINS pilot project which was developed and maintained at Government's cost (Rs 90 lakh) since its inauguration in December 1999 was handed over to the operator in January 2002 along with the assets for maintenance free of cost, though not provided in the agreement and without any specific order of the Government thereby conferring unintended benefit to the operator.</p>
	<p><i>v) Avoidable expenditure of Rs 72 lakh per annum due to outsourcing of personnel</i></p>	<p>As per the government orders while sanctioning TWINS expansion project, personnel required for handling transactions at each eSeva centre including DEOs be drawn from various participating departments/PSUs and surplus pool on deputation. However, out of 150 DEOs working in eSeva centres to end of March 2002, as many as 124 DEOs were outsourced (on contract basis) at the rate of Rs 4800 per month per DEO that too through two private agencies one of whom was the operator himself. Thus failure of the department to get required number of staff from the surplus pool resulted in outsourcing of personnel involving an avoidable expenditure of Rs 72 lakh per annum besides exposing the entire system to risk as huge cash was handled by contract personnel.</p>

### 3.2.8 Lack of supervision

**No system of monitoring the transactions entered outside office hours**

The Director, eSeva did not have access to the system but had to login only through application package which allows only a limited access to the user. No system of monitoring the activities of application users exists with the Director. Whenever the timings of the eSeva centre are to be extended due to exigencies of work, the timings were extended at Data centres by making necessary changes in the application. However, no record of extensions authorised was being maintained either manually or electronically. In the absence of such records, the authenticity and correctness of the transactions entered outside office hours could not be verified.

## **Conclusion**

Though Government launched a unique and conceptually a good project to put e-governance into action to provide a large number of services to the citizens on one stop shop basis, the programme suffered from lack of transparency, inefficient and ineffective implementation largely due to the unpreparedness of the participating departments/agencies.

Participation and co-ordination of the participating departments/agencies essential for achieving the goal was inadequate. The critical data and huge volumes of cash pertaining to various departments/agencies had been left to the administration of private operator without adequate internal controls. The network was exposed to serious risks of physical access controls and logical access controls. The single operator did not share any information on technical matters with the Director besides violating the contractual obligations. The monopolistic situation created had exposed the entire project and the participating organisations to serious risks. Data integrity, reliability and safety across the project were inadequate. Government needs to evolve a proper internal control mechanism to plug the security loopholes and strengthen the project.

The audit observations mentioned above were referred to the Government in August 2002. In an interim reply (August 2002), the Principal Secretary to the Government in IT&C department stated that eSeva was innovative and a new concept having no precedents and the progress was made through a constant process of experimenting.