Key Points of Report

Texas Department of Transportation
1994 Statewide Financial and Compliance Audit
March 1995

Overall Conclusion

The Department is not adequately protecting its automated resources by restricting access to the computer system and computer facilities. In fiscal year 1994, the automated system was used to process $1.6 billion in contractor payments. However, the Department has a system in place to ensure compliance with regulations for its largest federal program, Federal Highway Research, Planning and Construction ($1.3 billion). In addition, the Department's accounts that are significant to the statewide financial statements are accurate and properly reported. The accounts tested included federal revenues ($1.1 billion), expenditures ($2.9 billion), and interagency transfers ($1.9 billion).

Key Facts And Findings

- Access to the Department's automated resources is not adequately restricted. Security policies and procedures for maintaining the use of the computer resources are not always followed or enforced. In addition, log-on identification codes for terminated employees are not always deleted.

- Access to the main computer facility is not adequately controlled. In addition, responsibility for physical security of the computer facilities is not sufficiently assigned.

Table of Contents

Internal Control Issues

Internal Control Issue 1:
Restrict Access To Automated Resources

Access to the Department's automated resources is not adequately restricted. Security policies and procedures for maintaining the use of the computer resources are incomplete, and three systems are not adequately protected by the existing security policies and procedures.

Although the Information Systems Division has published some security policies for the mainframe, the following conditions were found:

· Formal policies and procedures for access security of personal computers, local area networks, and client server systems do not exist.

· Data in the output spool and system software manuals are not protected from unauthorized use.

· A risk assessment has not been done to determine the criticality and sensitivity of engineering systems.

Three systems, the Contract Information System, Human Resources Information System, and Automated Purchasing System, need improved security procedures to protect access to the information contained within them.

Restricting access to all computer systems will decrease the risk of unauthorized or accidental access, modification, or damage to computer resources. The Department relies on the computer for day-to-day operations, including the processing of $1.6 billion in contractor payments for fiscal year 1994.

Recommendation: Develop additional security policies and procedures to restrict access to the computer system:

· Develop security policies and procedures over local area networks, personal computers, and client server systems.

· Protect data in the output spool and systems software manuals from unauthorized use.

· Perform a risk assessment and implement security controls over engineering systems.

· Improve security procedures for the Contract Information System, Human Resources Information System, and Automated Purchasing System.

Management's Response: We concur that additional policies and procedures will decrease risk to computer resources in some instances. The Risk Analysis Project, scheduled to complete in September 1995, will provide information necessary to develop additional security procedures to restrict access to the computer system. An action plan will be implemented based on the Risk Analysis findings.

· *Policies and procedures for access security of TxDOT's local area networks, personal computers, and client servers will be* implemented *by December 31, 1995.*

· *The output spool issue has been addressed. On January 3, 1995, TxDOT Manual Notice 95-1 was issued to implement a computer job naming standard. Additionally, the software was implemented and controls defined to CA-Top Secret to provide for the protection of sensitive job output on the JES spool. We concur that the systems software manuals should be protected and badge reader locks will be installed by September 1, 1995.*

· *We concur with the issue on risk assessment and this issue will be addressed in the Risk Analysis project scheduled for completion in September, 1995.*

· *The Information Systems Division and the Office of Primary Responsibility (OPR) for Contract Information System (CIS) have discussed the potential security risk for that system. The OPR (the Construction and Maintenance Division) has chosen to accept the risk for this system. This decision will be reviewed after the Risk Analysis project is complete.*

We concur that security procedures should be improved for the Human Resources Information System (HRIS). A project is currently underway to restrict on-line access to the HRIS subsystems. This project is scheduled to be completed by May 1995.

The Automated Purchasing System (APS) consist of two major components: The Small Purchases (formally known as SPOT Purchases) and the American Software Inc (ASI) systems. Online access for both components is controlled by the Top Secret Security (TSS) System. The ASI systems also has it's own security system (AMSOFT security) which controls the functions that the users are allowed to perform. This is also controlled by TSS through the application control file.

The SMALL Purchases portion is in production and the programs are moved to production status by the Quality Assurance section. The Common Systems of ASI are in production, and the production libraries are not under the control of Quality Assurance at this time but an action plan will be developed to turn these and all future ASI production programs over to Quality Assurance.

Internal Control Issue 2:
Enforce Procedures Over Computer Log-On Assignments

Policies for computer log-on procedures are not always followed or enforced. Log-on identification codes of terminated and transferred employees are not always deleted or suspended. Group identifications are used for batch jobs, and the use of the CA-Top Secret Master Security Account is not monitored.

Lack of controls over computer log-on procedures may allow unauthorized and undetected transactions and may compromise the integrity of the computer systems.

Recommendation: Enforce policies and procedures for monitoring, deleting, and changing computer log-on assignments.

Management's Response: We concur with this issue and will implement steps for monitoring compliance with security procedures and the use of the Master Security Account by July 1, 1995.

Internal Control Issue 3:
Control Access To Computer Facilities

Access to the main computer facility at the Camp Hubbard location is not adequately controlled. The Department controls access by a card key system, door locks, and video camera surveillance. However, instances of unlocked doors and incomplete surveillance of doors were observed. In one instance, unimpeded access was made through two doorways directly into the computer room. In addition, two card key system readers were not working properly, and codes for terminated employees were not deleted.

Restricted access to the computer room reduces the risk of intentional or inadvertent damage to computer equipment. Unauthorized access could result in damage to equipment or data records.

Recommendation: Control access to computer facilities by ensuring that doors are locked, the card key reader system is working properly, and camera surveillance covers all appropriate entrances. Card keys for terminated employees should be deactivated.

Management's Response: The access problems stated in this issue have been corrected and a review of card key access will be conducted by Information Systems Division personnel on a yearly basis. The additional surveillance cameras will be installed by July 1, 1995. Procedures have been implemented to correct the problem of deactivating card keys for terminated employees.

Internal Control Issue 4:
Assign Responsibility For Physical Security

Responsibility for physical security at Camp Hubbard computer facilities is not sufficiently assigned. The job descriptions for two managers with responsibility for computer room operations do not clearly delineate security duties. In addition, responsibility for fire prevention systems and procedures and computer room access is not assigned.

Physical security responsibilities should be specifically assigned to ensure that necessary security procedures are performed. Clear responsibility would encourage managers to implement, follow, and enforce security procedures. Without appropriate assignment of responsibility, the risk increases that the physical security of the computer system will not be properly maintained.

Recommendation: Specifically assign the responsibility for computer room physical security. In addition, responsibility for physical security of the building and fire prevention systems should also be assigned.

Management's Response: We concur. The Manager of Computer Operation's job description will be updated to include responsibility for oversight of the physical security of all the operations area and the fire protection systems. This will be completed by March 31, 1995. The job description for the Manager for the Procurement and General Administrative Support Branch will be amended to reflect responsibility for Building Six security, excluding the Computer Operations area. This will be completed by March 31, 1995.

Federal Compliance Issues

The Department's most significant program, the *Federal Highway Research, Planning and Construction* program (CFDA 20.205), is funded by the U.S. Department of Transportation through the Federal Highway Administration. During fiscal year 1994, this program expended $1.3 billion for federally funded projects.

Recommendations addressed in other sections of this report could impact controls over federal funds, especially for the Department's most significant federal program.

Federal Compliance Issue 1:
Ensure Accuracy Of Accounting Records To Support Contractor Payments

The Houston and Fort Worth Districts are not ensuring accurate accounting records to support contractor payments. Inaccurate payments to contractors resulted from mathematical and posting errors and were not detected by project bookkeepers. No errors were noted in the Pharr District.

Our review covered 45 of the approximately 9,194 construction payments made during fiscal year 1994. The selected construction payments represent over $402 million of the

$1.3 billion in construction expenditures for federally funded projects. We noted errors on three construction projects. These errors have been corrected by the Department.

DISTRICT	PROJECT #	AMOUNT	TYPE OF ERROR
Fort Worth	NH 92 (83) M	$24,685	Overpayment
Houston	F 514 (102)	$12,505	Overpayment
Houston	IR 45-1 (267) 060	$44,460	Underpayment

Federal requirements state that program recipients are to maintain accurate accounting records. Recordkeeping procedures are designed to prevent, detect, and correct errors in a timely manner. They also provide for accurate contractor payments.

Recommendation: Ensure accurate accounting records to support contractor payments.

Management's Response: We concur with your recommendation. A recent process review of the Department's procedures for determination and documentation of pay quantities, conducted by the Federal Highway Administration, resulted in the following conclusions:

· *The Department has a very good system available for use by the districts for determination and documentation of pay quantities on active Federal-aid highway projects.*

· *The implementation of the processes/procedures by district project personnel is uniform and consistent.*

· *The system is satisfactory and no recommendations are made for improvement at this time.*

The above conclusions are based on an overall opinion on the implementation of the process. However, the Construction and Maintenance Division is developing a Construction Records Management training workshop to be conducted at the districts in an attempt to target the area offices and/or Districts that need help in this area. Furthermore, the Field Engineers in the Construction and Maintenance Division will continue to monitor these procedures as part of their project review process.

Federal Compliance Issue 2:
Submit Final Vouchers On A Timely Basis

The Department is not submitting final vouchers on a timely basis. Eight of the 45 final vouchers tested were submitted more than 12 months after the final acceptance date of the project. The Department completed 320 final vouchers in fiscal year 1994.
Title 23 of Code of Federal Regulations (CFR), *section 140.107* states that final vouchers are to be promptly submitted. Region VI of the Federal Highway

Administration (FHWA) has interpreted "prompt submission" to be within one year of the FHWA's final acceptance date of a project to the date the final voucher is paid.

Recommendation: The Department should submit final vouchers within the 12-month time frame required for "prompt submission."

Management's Response: There are three primary reasons that final vouchers are submitted later than one year after project completion:

a. The final clearance from the Federal Highway Administration has not been received.

b. There is insufficient federal apportionment to apply to the project, ie., we are waiting to free up some apportionment so we can collect all of the federal share of the project funding.

c. There is insufficient federal obligation authority to apply to the project, ie., we are waiting for obligation authority to become available so we can collect all of the federal share of the project funding.

The reasons noted in b. and c. should be mitigated in a few years due to the increased amount of funding now set aside for construction engineering and contingencies. In the future we will submit final vouchers within the one year time frame required for "prompt submission" when possible.

Audit Scope

The primary focus of our audit was the Department's financial and administrative controls over the *Federal Highway Research, Planning and Construction* program ($1.3 billion) relating to the State's transportation system. We gained an understanding of the internal control structure, including general control environment, controls over federal billing, cash disbursements, payroll indirect costs, and the federal program. Specific procedures were used to test compliance with the major federal program. We gained an understanding and tested general controls over automated operations. Certain financial accounts were also tested, including federal revenues ($1.1 billion), expenditures ($2.9 billion), and interagency transfers ($1.9 billion).