
Secretary of State

State of Oregon

OREGON DEPARTMENT OF TRANSPORTATION

General Computer Controls



Audits Division

Secretary of State

State of Oregon

OREGON DEPARTMENT OF TRANSPORTATION

General Computer Controls



Audits Division

OFFICE OF THE
SECRETARY OF STATE
Phil Keisling
Secretary of State
Suzanne Townsend
Deputy Secretary of State



AUDITS DIVISION
John Lattimer
Director

(503) 986-2255
FAX (503) 378-6767

Auditing for a Better Oregon

The Honorable John Kitzhaber, M.D.
Governor of Oregon
State Capitol Building
Salem, Oregon 97310

Grace Crunican, Director
Oregon Department of Transportation
355 Capitol Street NE
Salem, Oregon 97310

This report includes our evaluation of the general computer controls in place at the Oregon Department of Transportation (ODOT) data center. During this audit, we reviewed procedures relating to physical security, logical access control, backup and recovery, contingency planning, and other organizational responsibilities. We also reviewed the status of related recommendations contained in our previous audit of the data center's general controls.

This report includes recommendations intended to improve data center operations. On February 26, 1999, the governor signed Executive Order Number EO 99-05. The order directed the operational alignment of the Department of Administrative Services and the ODOT data centers. Therefore, the recommendations contained in this report should be considered and implemented during this transition process. The Oregon Department of Transportation generally agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
April 21, 1999

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	vii
INTRODUCTION	
Information Technology Controls	1
Scope and Methodology	2
AUDIT RESULTS	
Ensuring System Security	5
Organizational Structure	9
Ensuring Continuous Service	11
Managing Facilities	12
PRIOR AUDIT FINDINGS	15
COMMENDATION	17
AGENCY'S RESPONSE TO THE AUDIT REPORT	19

SUMMARY

PURPOSE

The purpose of our audit was to evaluate general controls at the Oregon Department of Transportation (ODOT) data center. General controls are those controls intended to protect the environment in which the software applications process data. These control procedures relate to physical security, logical access, backup and recovery of data, contingency planning, and other organizational responsibilities.

BACKGROUND

The Information Systems Branch operates ODOT's data center. The data center provides data processing and support services to all programs within ODOT. In addition it provides services to other governmental agencies and organizations such as the Forestry Department, Parks and Recreation Department, Oregon State Police, and several cities and counties. On February 26, 1999, the governor signed Executive Order EO 99-05 directing the operational alignment of the Department of Administrative Services data center with the ODOT data center.

RESULTS IN BRIEF

The ODOT data center can improve its controls governing data center operations.

RECOMMENDATIONS

ODOT, in conjunction with the Department of Administrative Services (DAS), should consider the following priority items during the alignment of their data centers:

- Improve logical access controls and establish policies and procedures to ensure that access rights are appropriately administered and maintained.
- Ensure that the organizational structure of the data center provides separation of important duties. The structure should isolate system programming duties from application development and programming functions. In addition, ensure that staffing is sufficient during all shifts to provide adequate safety, supervision, and separation of duties.
- Fully develop and test the data center's disaster recovery and contingency plans.

- Further restrict physical access to the data center and improve processes to ensure control over access. In addition, develop procedures to ensure emergency preparedness training and monitoring of environmental systems occur. Also, improve control over sensitive inventory.

AGENCY RESPONSE

The Oregon Department of Transportation generally agrees with our recommendations. The department's full response can be found on page 19 of this report.

INTRODUCTION

The Technology Management section of the Oregon Department of Transportation (ODOT) Information Systems Branch (ISB) operates the department's data center. ISB is a service organization within ODOT's Central Administration structure funded by a combination of rates charged for services provided and assessments to line organizations. ISB provides data processing, data management, application development, technology support, information management, voice and data communications, and consultation services to all programs within ODOT. It also provides services to other governmental agencies and organizations such as the Forestry Department, Parks and Recreation Department, Oregon State Police and several local cities and counties. The services provided by the data center directly support the program services delivered to ODOT clients such as vehicle registration and licensing. In addition, the center processes transactions for important applications such as the Transportation Environment Accounting and Management System (TEAMS).

On February 26, 1999, the governor signed Executive Order Number EO 99-05. The order directed the operational alignment of the Department of Administrative Services and the ODOT data centers. Therefore, the recommendations contained in this report should be considered and implemented during this transition process.

INFORMATION TECHNOLOGY CONTROLS

Information technology controls are typically classified as general controls or application controls. General controls protect the environment in which software applications process data. These controls focus on procedures pertaining to organization and relationships, managing facilities, system security, providing continuous services, managing operations, managing resolution of problems and incidents, and compliance with external requirements of individual software applications. Application controls relate to specific requirements of individual software applications. They are designed to reduce the risk of errors in recording, processing, classifying or summarizing of authorized transactions. Application controls ensure that a specific software application's data input, processing, and output functions occur as intended.

General controls coupled with application controls provide the level of assurance that the transactions processed through the system are authorized, reliable and complete. It is the responsibility of ODOT's Technology Management section to ensure that data center general controls are sufficient to provide an appropriately secure

operating environment to protect ODOT's computer applications.

SCOPE AND METHODOLOGY

Our audit included a review of Technology Management section's information systems general controls. We performed our fieldwork between November 1998 and April 1999. This work included a review of the control procedures operating during the specified time period for the following information technology processes:

- Organizational structure
- Managing operations
- Managing problems and incidents
- Ensuring continuous service
- Managing facilities
- System security
- Ensuring compliance with external requirements

The objective of our audit was to evaluate the adequacy of Technology Management's general controls at the ODOT data center. Our audit work included inquiries of Technology Management's personnel, examination of documents supporting controls and procedures, and observation of Technology Management's control processes and operations. We evaluated compliance with applicable laws, rules, and regulations pertaining to internal controls and the operation of the data center. We also reviewed the status of findings noted in our previous audit report on the data center, which was issued in 1995. In addition, we reviewed the status of the data center's year 2000 remediation efforts. During our audit we used the Information Systems Audit and Control Foundation's (ISACF) "Control Objectives for Information and Related CobiT) to identify generally accepted and applicable internal control objectives and practices for information systems. ISACF is a worldwide organization dedicated to research, develop, and publicize generally accepted information technology control objectives and audit guidelines.

We conducted our audit according to generally accepted government auditing standards. We limited our review to

the general controls specified above as they applied to the operations of the ODOT data center.

AUDIT RESULTS

ENSURING SYSTEMS SECURITY

The Oregon Department of Transportation (ODOT) relies on various manual and automated controls to safeguard data processed through its data center against unauthorized use, disclosure or modification, and damage or loss. However, those controls could be improved to better ensure systems security. Areas needing improvement include security software configuration, providing access according to user's needs, management and monitoring of access privileges, and security policies and procedures. These conditions exist because ODOT managers have not ensured correction of known weaknesses. As a result, the data center is less able to ensure the integrity of its systems and data.

Security Software Configuration

Access to computer resources should be restricted and controlled by mechanisms, such as password protection, to identify and validate users and control their access to computing systems. Procedures should be in place to ensure the effectiveness of these mechanisms.

ODOT uses the software program Resource Access Control Facility (RACF) to restrict access to systems, data, and programs stored on its mainframe. The effectiveness of RACF depends on whether it is properly implemented and maintained. Several weaknesses exist in the data center's RACF configuration. Those conditions include the following:

- Some employees are authorized to share a single user ID and some have more than one assigned user ID. Both of these conditions make it difficult to monitor and control employee access and activity.
- Timeout features, which are designed to automatically terminate user connections when they are inactive for a period of time, are not effectively utilized.
- Data center management assigned conflicting access attributes to two user IDs. These employees had "special" and "auditor" attributes, contrary to RACF

specifications. According to the RACF Auditor's Guide, those access attributes should not be assigned to the same individual so that an appropriate separation of duties is maintained.

Providing Access According to Users' Needs

ODOT managers should authorize logical access to computer resources based on users' needs to view, add, change or delete data. In many instances, ODOT management assigned access privileges that exceeded what was needed for employees to perform their assigned duties or what was appropriate to ensure adequate separation of duties. Examples of improper access to data or programs includes the following:

- Technical support employees have access to application programs, data files, and to the encrypted password file.
- Some application programmers have access to operating system files.
- One user ID was configured to allow maximum access to the entire ODOT mainframe. This ID and its password are not assigned to a specific employee, but are intended to be used by operators or other technicians to resolve unforeseen service disruptions. In addition, this ID and password were recorded and filed in an unsecured location within the data center.
- Some former data center employees still had certain RACF access privileges assigned to them even though their new duties no longer required that level of access.

Management of Logical Access Privileges

CobiT recommends that management should have processes in place to periodically review and confirm access rights. It further recommends that organizations regularly log, report, and review security activities and adjust their efforts to identify and resolve incidents or problems involving unauthorized attempts to use computing resources or individuals' mistaken attempts to access authorized resources.

ODOT security services do not have processes to periodically evaluate logical access privileges for ODOT employees to ensure they remain appropriate for current work assignments. In addition, data center management does not independently review security reports to ensure that monitoring and timely resolution occurs for reported security incidents or suspicious user activity.

Security Policies and Procedures

CobiT indicates that controls should also be in place to manage security in a central manner to provide consistent and efficient global access control. These controls should provide timely and effective maintenance of user access privileges in line with business requirements.

ODOT's written security policies and procedures are not always consistent with best practices. For example, the policies and procedures do not promote periodic agency-wide training and awareness of security issues or require employees to sign security and confidentiality agreements. In addition, they allow users to share passwords with helpdesk personnel and security administrators to facilitate routine maintenance of personal computers.

ODOT should also improve its procedures for assigning new employees access to computing systems. Under current methods, requests for access come from various sources including employees, fellow workers, or employees' supervisors. The Computer Security Unit processes these requests and mails the resulting IDs and passwords to the employees' supervisor. Supervisors are responsible for concurring whether an employee should be given access to the system. If the supervisor agrees with the action, he or she is instructed to pass the envelope containing the password and ID to the employee. This process has the following weaknesses:

- Supervisors responsible for deciding whether access should be given to their employees do not know whether access was actually granted according to the employees' needs to view, add or modify data.
- It does not ensure that employees are aware of their responsibilities for system security prior to receiving access to the system.

- New user IDs and passwords are not delivered directly to employees receiving access.

System access controls are further weakened because helpdesk and operations employees reset passwords but do not maintain documentation of these security maintenance activities. In addition, the data center does not have procedures to ensure that user IDs of temporary employees, terminated employees, other non-agency users, or training IDs are timely revoked when access is no longer needed. The Computer Security Unit did not delete approximately 100 user IDs that were assigned but never used.

Recurring Access Control Issues

Many of the above issues were also noted in our 1994 audit of the data center. They continue to exist because ODOT does not provide clear policies and procedures or managerial oversight over system security functions. Thus, ODOT is less able to protect its systems, data, and programs from unauthorized use, disclosure or modification, and damage or loss.

We recommend that Information System Division managers ensure that the following measures are taken to improve system security:

- Develop and implement policies and procedures to ensure that all employees have unique user IDs. All user IDs not specifically assigned to an employee should be removed from the system.
- Use timeout features to automatically terminate user connections when they are idle for more than 30 minutes. For systems processing sensitive or confidential information ODOT should consider terminating connections when they are idle for 15 minutes.
- Remove RACF user attributes that conflict with RACF Auditor's Guide recommendations.
- Establish policies and procedures to ensure that logical access is based on users' needs. These policies should ensure that appropriate separation of important or critical functions is maintained. All user IDs having excessive access privileges should be resolved.

- Develop and implement policies and procedures to require periodic evaluations of access privileges and to independently review security reports.
- Promote and facilitate agency-wide system security training and awareness of security issues. In addition, management should develop policies requiring users to sign security and confidentiality agreements.
- Require that users not reveal their passwords to other employees.
- Develop and implement policies and procedures to ensure that access requests are authorized and appropriate prior to set-up. In addition, these policies should provide for secure and confidential communication of user IDs and initial passwords.
- Develop and implement procedures to timely revoke user access when it is no longer required.

ORGANIZATIONAL STRUCTURE

ODOT management is responsible for maintaining an appropriate operating environment within its data center. These responsibilities include providing appropriate staffing and assignment of responsibilities to ensure separation of important operating functions. Separation of duties is important to minimize the likelihood of errors or illegal acts occurring and to assure that if such events do occur, they will be detected and corrected timely. In that respect, Department of Administrative Services (DAS) guidelines recommend that two or more employees should be on duty at all times, and that employees working in sensitive positions should periodically rotate to other responsibilities. DAS policy further recommends that employees performing systems development should not be involved in developing application programs. CobiT standards also recommend that system and application programming functions remain separate to limit the opportunity for a single individual to subvert a critical process. It further stresses that system programmers should not have access to production databases, application programs or data files in

order to maintain acceptable levels of security. The current organizational structure at the ODOT data center does not adequately address these issues. In addition, data center staffing at times is not sufficient to ensure adequate supervision or separation of sensitive tasks.

Segregation of Duties

ODOT's organizational structure does not always support adequate separation of important or sensitive functions according to best practices. For example, when problems arise, technical support employees who normally perform systems programming tasks sometimes assist in application program development and program support. In the event that this support will be needed, they have access to sensitive system files and utilities and application programs and data files. Operations and helpdesk staff also perform some system security duties, which is contrary to best practices.

The above conditions exist because data center management allows experienced system programmers to perform various tasks even when they are not within the scope of the employees' positions. Further, management does not have security policies or procedures in place to prohibit system programmers from gaining logical access to application files and programs. This situation increases the likelihood that unauthorized or inappropriate changes could be made to data or application programs, and go undetected.

Data Center Staffing

The data center operates 24 hours a day, seven days a week. Since production work is not performed on weekend shifts, data center management provided only minimal staffing for those shifts. During some weekend shifts only one employee, an operator, staffs the data center. Because of the lack of supervision and monitoring, the risk increases that errors or illegal acts could occur and go undetected for extended periods of time. In addition, operators working alone on weekend shifts are isolated and may not receive timely assistance should they encounter health or safety problems.

We recommend that the Information Systems Branch (ISB) restrict system programmers' access to include only those regions necessary to carry out the system programming duties. In addition, system programmers

should be excluded from providing application programming services or support. We also recommend that ISB management provide more adequate staffing of the data center for weekend shifts.

ENSURING CONTINUOUS SERVICE

Disaster recovery and contingency planning are necessary to ensure that services will be provided in the event of a disruption. CobiT recommends that management ensures that a written disaster recovery and contingency plan is developed, tested, maintained and that all concerned parties receive regular training on their roles and responsibilities. DAS Information Resource Management Division (IRMD) policy also requires state agencies to develop and maintain disaster recovery and contingency plans for their information systems.

ODOT's Technology Management section is responsible for developing and maintaining a working disaster recovery plan for the data center. During our 1994 audit of the data center, we noted that ODOT's disaster recovery plan was not fully developed. At that time many of the elements required for a successful recovery of critical data were not current or were missing from the plan. Furthermore, a written contingency plan was not developed.

During our current audit, we noted that this condition continues to exist. Many of the required elements for the successful recovery of critical data were not included in the plan and many necessary elements were not current. The following weaknesses currently exist:

- The lists of disaster recovery team members are not current. Some listed team members no longer work at ODOT. Further, the remaining team members were not trained and do not have written descriptions outlining their roles and responsibilities.
- The off-site storage location does not have many of the required resources needed for a successful recovery program. Missing items included information such as a list of the names and phone

numbers of team members and lists of key resources such as operating manuals, program documentation, equipment and supplies, and contracted service providers.

- Processes do not exist to ensure that backup tapes remain usable.
- The plan has not been tested since 1996. This test only included recovery of the operating system and other necessary rehearsals were not performed.

These conditions exist because the Technology Management section has not devoted sufficient resources or managerial oversight to fully developing and maintaining its disaster recovery plan. As a result, ODOT's ability to respond to disruptions in service is lessened. Thus, critical systems could be inoperable for a longer period in the event of a disaster.

We recommend that ODOT's Technology Management section, in conjunction with management from the Department of Administrative Services General Government Data Center, fully develop and test disaster recovery and contingency plans for the data center. In addition, we recommend that management ensure that staff members are sufficiently aware of and trained in their individual responsibilities under those plans.

MANAGING FACILITIES

Controls to manage facilities help to safeguard assets and people against man-made and natural hazards. These controls should include measures to limit physical access to the data center, ensure that the data center's environment is appropriate for computer operations, and ensure the safety of those working in the center. Areas needing improvement include measures to limit physical access, safeguard sensitive documents, and provide emergency preparedness training and maintenance of environmental monitoring systems.

Physical Access Controls

ODOT uses computer controlled key-card locks to limit access to its data center. The DAS Facilities Division maintains this system. The Technology Management

section is responsible for coordinating with DAS Facilities Division to ensure that access to the data center is limited to authorized staff; however, we noted key-card access to the data center was not appropriately restricted. For example, of the 254 persons having access, nine were Oregon State Police employees no longer working in the area and 57 were ODOT employees who no longer needed the access to perform their duties. Furthermore, 153 of the key cards were issued to DAS staff and its vendors.

These conditions exist because ODOT does not adequately monitor or control key-card issuance. Inadequate monitoring increases the risk that inappropriate or unnecessary access privileges will be granted, thus increasing the risk of unauthorized intrusion.

Safeguarding Documents

Managing facilities also includes safeguarding sensitive documents. The ODOT data center prints various sensitive documents including motor vehicle titles and tags. Print stock for these documents are kept in storage cabinets in the data center. Computer operators track custody and use of these documents using a "Sensitive Inventory Issues Report". Those reports included gaps in the numbering sequences that indicated some documents were not accounted for. Data center personnel also keep the keys to the storage cabinets in another unlocked storage cabinet during the swing and graveyard shifts.

ODOT management has not ensured that the Sensitive Inventory Issues Report was completed and that non-reconciling items were resolved. In addition, it has not assigned responsibility for securing the sensitive document inventory.

Emergency Preparedness Training

The data center depends on emergency equipment such as fire extinguishers to provide protection in the event of a fire. However, management has not provided periodic training on how to use the emergency equipment. Data center staff members indicated that training was last provided for data center employees in 1993. As a result, data center staff may be less prepared to respond to an emergency, should one occur.

Environmental Monitoring Systems

The data center does not have procedures to ensure that environmental monitors and fire suppression systems are maintained and working according to specifications. ODOT managers delegated responsibility for maintaining the environmental monitoring systems to the DAS Facilities Division; however, the data center had not documented whether these services were performed. In addition, data center managers were unaware whether fire suppression systems, smoke detectors, and humidity/temperature monitors were serviced and tested. The above factors increase the risk that important environmental and safety monitoring systems may not be functioning as intended and thus may not be able to detect hazardous conditions should they occur.

We recommend that ODOT's Information Systems Division in conjunction with the Department of Administrative Services make the following improvements to facilities management:

- Develop and implement procedures to more adequately monitor and control key card access privileges. These procedures should include regular verification that only personnel having responsibilities within the data center have access.
- Establish written procedures to ensure that the *Sensitive Inventory Issues Report* is complete and that non-reconciling items are resolved. In addition, assign the responsibility for securing sensitive inventory and ensure that keys to sensitive inventory storage cabinets are safeguarded.
- Provide regular emergency preparedness training to data center staff.
- Assign responsibility for ensuring that environmental and safety monitors are maintained on a regular basis and that appropriate records are kept of maintenance performed.

PRIOR AUDIT FINDINGS

This section summarizes Oregon Department of Transportation efforts to resolve prior audit findings included in our report titled *State of Oregon, Oregon Department of Transportation, Review of Computer Center Controls, July 1, 1992, to April 30, 1994*.

Prior Audit Recommendations	Disposition
1. Improve key card access controls and procedures including reconciliation of authorized users, timely maintenance of the key card database and procedures for issuing and revoking key cards.	Not implemented. See page 12.
2. Prepare written procedures for controlling printing and handling of sensitive documents.	Partially implemented. See page 13.
3. Follow the department's separation and exit policies and procedures.	Implemented.
4. RACF coordinator should periodically monitor various attributes assigned to users and re-evaluate access needs when user's responsibilities change. Also, review the operating system data sets and remove unnecessary access capabilities.	Partially implemented. See page 6.
5. Develop policy to prohibiting user IDs that are not specifically assigned to one individual or assigning multiple user IDs to one individual unless specifically warranted.	Partially implemented. Policies have been developed but not fully implemented. See page 5.
6. Maintain documentation of security activity follow up.	Implemented.
7. Enforce policy requiring RACF training.	Implemented.
8. Implement procedures to ensure users periodically change passwords.	Implemented.
9. Policies and procedures requiring use of RACF.	Implemented.
10. Security reports should be reviewed to ensure that controls are functioning properly and to detect unusual events.	Partially implemented. See page 6.
11. Require a time-out feature for all new systems and all systems with sensitive information.	Not implemented. See page 5.
12. Operators have "read only" capability in RACF-controlled libraries or data sets.	Not implemented. See page 6.
13. Compare the SMF IPL log to the "Morning Report" to ensure that all recorded and adequately explained.	Implemented.
14. Provide compensating controls to monitor work performed by employees during weekend shifts.	Not implemented. See page 10.

Prior Audit Recommendations	Disposition
15. Review the disaster recovery plan at least annually and update as necessary. Also, perform periodic tests of the plan, provide training, and provide for an alternate processing site.	Not implemented. See pages 11 and 12.
16. Request all user agencies to identify critical files to be backed up and stored off-site. Also, consider taking backed up files to the off-site location more frequently.	Implemented.

COMMENDATION

The courtesies and cooperation extended by the officials and employees of the Oregon Department of Transportation during the course of our investigation are very commendable and are sincerely appreciated.

AUDIT TEAM

Sharron E. Walker, CPA, CFE
Ann Waterman, CPA
Neal E. Weatherspoon, CPA, CISA
Stanley Mar
Pamela Stroebel, CPA
Ann Takamura

AGENCY'S RESPONSE TO THE AUDIT REPORT



Oregon

John A. Kitzhaber, M.D., Governor

Department of Transportation

Office of the Director

355 Capitol St. NE

Rm 135

Salem, Oregon 97301-3871

September 16, 1999

FILE CODE:

Sharron E. Walker, Deputy Director
Office of the Secretary of State, Audits Division
255 Capitol Street N.E., Suite 500
Salem, OR 97310

Dear Ms. Walker:

Following is our response to the Secretary of State's Audit, General Computer Controls.

This response addresses the audit findings from the ODOT Data Center audit conducted from November 1998 through April 1999. Initially, we will comment on the findings in general, then address specific findings we are unable to substantiate. Lastly, we will document current and prior audit findings that have been corrected.

General Comments

We concur with the vast majority of individual findings in the audit draft. Although improvements to the noted areas are taking place, Data Center management has completely turned over in the last 18 months, slowing some of our efforts. We appreciate the detailed work completed by the audit team. Their attention to detail has identified to these new and interim managers additional areas needing improvement. Our goal is to provide the best service possible to ODOT business lines, while providing a secure computing environment.

As noted in the audit summary, Executive Order Number EO 99-05 directs the operational alignment of the Department of Administrative Services (DAS) and the Oregon Department of Transportation (ODOT) data centers. It is our intent to study the recommendations noted in the audit draft and plan for implementation during the transition of the ODOT Data Center to DAS. (The projected date of the data center alignment is approximately April – June 2000.) As a result, we will need to work closely with DAS management to ensure that corrected procedures are implemented and specifically addressed by policy. Since the combined data center will be a function within DAS itself, DAS will ultimately be responsible for maintaining the corrected findings, as noted in the audit draft.

Specific Findings Contention

Ensuring Continuous Service (page 11, third bullet) – “Backup tapes are not regularly tested for usability.”



Sharron E. Walker
September 16, 1999
Page Two

Data Center backup tapes are rotated off site, daily, and recalled frequently to retrieve data. Full volume backups are rotated on a weekly basis through the offsite storage facility. In the event of a disaster recovery scenario, data will be restored from these full volume backups.

Current Audit Findings - Rectified

Providing Access According to User's Needs (page 6, third bullet) – “In addition, this ID and password were recorded and filed in an unsecured location.”

The container holding this ID and password have since been moved from the document where they were stored (which was kept within a controlled environment) to a locked storage cabinet in a controlled environment.

Ensuring Continuous Service (page 11, first paragraph) – “Disaster recovery and contingency planning are necessary to ensure that services will be provided in the event of a disruption ...a written contingency plan was not developed.”

In late May 1999, the Data Center Disaster Recovery books were produced. They contain current contacts, hardware/software configurations, response teams, and team procedures. ODOT, in conjunction with DAS, is currently constructing a Request For Proposal (RFP) for an alternate recovery site that will meet the needs of the consolidated data centers. An award is expected early in 2000, and a live test will be conducted shortly thereafter.

Emergency Preparedness Training (page 13, last paragraph) – “However, management has not provided periodic training on how to use the emergency equipment. Data Center employees indicated that training was last provided for data center employees in 1993.”

The fire suppression system vendor provided training to Computer Operations personnel in June 1999.

Security Software Configuration (page 5, third bullet) – “Timeout features, which are designed to automatically terminate user connections when they are inactive for a period of time, are not effectively utilized.”

With the completion of the “NT rollout” project, end user terminals are configured to timeout after 15 minutes of nonuse. Currently, the machines at DMV are configured to disallow changes to this setting, however changes may be made to this setting on all other machines. Removal of this option is being forwarded for senior management approval with the actual removal expected in late 1999.

Sharron E. Walker
September 16, 1999
Page Three

Providing Access According to Users' Needs (Page 6) – “In many instances, ODOT management assigned access privileges that exceeded what was needed for employees to perform their assigned duties or what was appropriate to ensure adequate separation of duties.”

As a result of the imminent “merge” with the DAS Data Center, the need to minimize staff to ensure integrity of the new data center has necessitated a less than full staff at times. ODOT has weighed the risks and costs associated with this posture and determined the lesser risk to exist in the current structure. If the consolidation is not forthcoming, staffing levels will be increased.

Prior Audit Findings – Rectified

Item #1 (page 17)

The *Procedure for Revenue Building Door Cards – ODOT Information Systems Section* was created in January 1999. The procedure is in final draft form and expected to be finalized shortly.

Item #2 (page 17)

Written procedures for logging the sensitive and controlled documents on the Sensitive Inventory Issues Report, as well as the ODOT Secured Documents Control Log, were completed and issued in May 1998.

Item #5 (page 17)

This prior recommendation has indeed been implemented. Reference: ODOT Policy ADM 05-05, ODOT Computer Security Policy Guidelines, Chapter 2, Section 2.1.

Item #11 (page 17)

See Security Software Configuration in the **Current Audit Findings – Rectified** section above.

Item #12 (page 17)

In an effort to provide better customer service to ODOT employees at no additional cost to taxpayers, ODOT Data Center operators have taken on tasks and duties not traditionally associated with their positions. These duties sometimes require access to programs, files or libraries at levels other than “read only”.

If this effort is successful, a review of the ODOT operator position description will follow.

Item #14 (page 17)

The majority of tasks performed by operators on weekends are submitted by automation, and progress as a direct result of operator interaction. Logs and

Sharron E. Walker
September 16, 1999
Page Four

records of jobs run, tapes mounted, forms printed, etc. are automatically created, periodically audited for errors, and can be reviewed as circumstances dictate.

Item #15 (page 18)

See Ensuring Continuous Service in the **Current Audit Findings - Rectified** section above.

If you have questions, please call Marc Williams at 986-4382. Thank you.

Sincerely,

A handwritten signature in cursive script that reads "Mike Marsh".

Mike Marsh, Executive Deputy Director

Copies to:

Grace Crunican
Dave White
Marc Williams

FACTS ABOUT THE SECRETARY OF STATE AUDITS DIVISION

The mission of the Audits Division is to “Protect the Public Interest and Improve Oregon Government.” The Oregon Constitution provides that the Secretary of State shall be, by virtue of his office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

DIRECTORY OF KEY OFFICIALS

Director

Deputy Director

Deputy Director

John N. Lattimer

Catherine E. Pollino, CGFM

Sharron E. Walker, CPA, CFE



This report, which is a public record, is intended to promote the best possible management of public resources.

If you received a copy of an audit and no longer need it, you may return it to the Audits Division. We maintain an inventory of past audit reports. Your cooperation will help us save on printing costs.

Oregon Audits Division
Public Service Building
Salem, Oregon 97310

503-986-2255

We invite comments on our reports through our Hotline or Internet address.

Hotline: 800-336-8218

Internet: Audits.Hotline@state.or.us

<http://www.sos.state.or.us/audits/audithp.htm>

Auditing to Protect the Public Interest and Improve Oregon Government