

**REPORT BY THE
AUDITOR GENERAL
OF CALIFORNIA**

**THE OFFICE OF STATE PRINTING NEEDS
TO STRENGTHEN CONTROLS OVER ITS
ELECTRONIC DATA PROCESSING RESOURCES**

**The Office of State Printing Needs
To Strengthen Controls Over Its
Electronic Data Processing Resources**

T-973, July 1991

**Office of the Auditor General
California**



Kurt R. Sjoberg, Auditor General (acting)

State of California
Office of the Auditor General
660 J Street, Suite 300, Sacramento, CA 95814
Telephone : (916) 445-0255

July 25, 1991

T-973

Honorable Robert J. Campbell, Chairman
Members, Joint Legislative Audit Committee
State Capitol, Room 2163
Sacramento, California 95814

Dear Mr. Chairman and Members:

The Office of the Auditor General presents its report concerning the Office of State Printing's controls over its electronic data processing resources. The report indicated that the Office of State Printing (OSP) needs to improve its disaster recovery capability. In addition, the OSP needs to strengthen controls over changes to its computer programs. Further, the OSP needs to improve controls that prevent unauthorized access to its computer programs and information databases. And, finally, the OSP needs to better document its computer applications.

Respectfully submitted,

A handwritten signature in cursive script that reads "Kurt R. Sjoberg".

KURT R. SJOBERG
Auditor General (acting)

Table of Contents

Summary		S-1
Introduction		1
Chapter 1	The Office of State Printing Needs To Strengthen Its Disaster Recovery Planning at Its Electronic Data Processing Department	5
	Recommendations	9
Chapter 2	The Office of State Printing Needs To Strengthen Controls Over Changes to Its Computer Programs	11
	Recommendations	17
Chapter 3	The Office of State Printing Needs To Strengthen Security Over Its Electronic Data Processing Resources	19
	Recommendations	26
Chapter 4	The Office of State Printing Needs To Better Document Its Computer Systems	27
	Recommendations	30
Response to the Audit	State and Consumer Services Agency Department of General Services	31

Summary

Results in Brief During our audit of the electronic data processing (EDP) department of the Office of State Printing (OSP), we determined that the EDP department needs to strengthen its preparation for disaster. Also, it needs to improve certain controls because it and its computer programs and information databases are susceptible to unauthorized access, as well as other abuses. We noted the following conditions:

- The OSP has not installed water detectors despite flooding on two occasions and has a closed-off drain pipe that presents a hazardous situation;
- The OSP can improve controls over its computer program changes, making itself less susceptible to undocumented and unauthorized changes;
- The OSP can strengthen controls over access to its computer systems, thereby reducing the systems' vulnerability to unauthorized access and misuse; and
- Some of the OSP's computer systems are undocumented or poorly documented, putting programmers and nontechnical users at a disadvantage in maintaining and understanding those systems. Some information from these systems may be unreliable.

Background The OSP, which is one of 22 offices in the Department of General Services, provides printing services for the executive, legislative, and judicial branches of state government, the state university and colleges, and other state agencies. Legislative work alone comprises 15 percent of the work load. The OSP is funded by charges to the agencies served. Annual sales exceed \$50 million dollars.

The EDP department provides essential data processing services to all of the OSP's departments as well as other state agencies. Primary OSP users of the EDP department include the material control, estimating, accounting, and production control staff. The EDP department's major computer systems consist of the following: the stock inventory system, estimating system, payroll system, production control system, accounting system, and legislative bill room system. In addition, the OSP maintains telecommunication links with the Legislative Data Center and the Stephen P. Teale Data Center to transfer data into the OSP's composition department.

**The OSP
Needs To
Strengthen
Its EDP
Disaster
Recovery
Planning**

The OSP's computer systems are important assets, ones that must be protected and safeguarded against disaster if they are to consistently operate to service the information needs of the OSP. The first step to protecting these assets is to identify the risks to them to determine where they are vulnerable. Once the risks are analyzed, management has the necessary information to make intelligent decisions about the selection of cost-effective security measures. However, the OSP has not taken adequate measures to detect and prevent floods in the computer room and its subfloor. In addition, the OSP's operational recovery plan did not contain sufficient procedures to effect a recovery following a disaster or plans for an alternate processing site if the computer room became inoperable.

**The OSP
Needs To
Strengthen
Controls
Over Changes
to Its
Computer
Programs**

For most computer systems, programmers must periodically make changes to improve or correct computer programs. These changes to the programs should be controlled through a structured process. Controlling changes made to computer programs is necessary to ensure that they are authorized, designed, documented, and implemented as intended by the requestor of the change, usually the user or data processing management. If program changes are uncontrolled, there is less assurance that the computer systems will function correctly, increasing the risk of invalid management information.

However, the OSP does not always follow a structured process when making program changes. For example, we found program changes that were made without any request documents showing that the changes had been requested, authorized, tested, or implemented. In addition, we found one instance where the changed version of the program was left unprotected and susceptible to further changes of either an accidental or intentional nature. Moreover, we noted that the OSP has not adequately separated the responsibilities for making changes to computer programs and for installing those changes. When the OSP fails to separate duties, it is susceptible to unauthorized changes being made without detection.

**The OSP
Needs To
Strengthen
Security
Over Its
Electronic
Data
Processing
Resources**

Security controls are the protective measures that are used by an EDP facility to reduce the possibility of loss, disruption, or harm to computer programs, information databases, and computer equipment. Security controls protect EDP resources through a combination of access controls, administrative procedures and policies, and software and hardware controls.

Contrary to State Administrative Manual requirements and some of its own policies, the OSP has not employed adequate security controls over its computer programs, information databases, and computer equipment. Specifically, the OSP has inadequate security controls to regulate access to its computer systems by unauthorized individuals from other agencies outside

the OSP. Also, the OSP does not require adequate accountability from users of its computer systems. Specifically, the OSP did not password protect critical programs that allow access to and operation of its computer systems. In addition, we found that two software products in use at the OSP inadvertently allow programmers the authority to change computer programs and information databases without approval. Furthermore, the OSP has not restricted access to its computer room to those employees with compatible duties. Finally, we found that nearly everyone in the OSP is allowed to access the computer systems through terminals without a user identification or password. Some of these terminals allow users to add or alter data in various applications. As a result of these weaknesses, the OSP has increased its vulnerability to inappropriate program changes, disclosure of sensitive data, and misuse of its computer systems.

**The OSP
Needs To Better
Document Its
Computer
Systems**

Development of new computer systems should include the preparation of detailed documentation for the operation and control of the system. Effective documentation describes the systems and procedures for performing data processing tasks and serves as a source of information for the systems' technical and nontechnical users. To be effective, documentation should be prepared according to established standards. Whenever changes are made to computer systems, the documentation should be updated to reflect those changes.

However, some of the OSP's computer systems are undocumented or poorly documented. For example, we found that, for some of its computer systems, the OSP inadequately described the functions the systems perform, the processes the systems go through, and the reports the systems produce. Moreover, we found that poor documentation for another system prevented users from reconciling differences between two sets of cost accounting information. However, according to the EDP manager, this system will be replaced with a new one in the near future.

Recommendations

To improve its ability to recover from a disaster, the Office of State Printing should take the following actions:

- Ensure that water or other fluids can be detected and removed from the computer room and its subfloor; and
- Further develop and refine its operational recovery plan.

To strengthen its program change process, the OSP should take the following actions:

- Ensure that all program changes are documented to show they are requested, approved, tested, and authorized for implementation before they are accepted into production;
- Ensure that changed versions of programs are not left unprotected and susceptible to further changes without authorization; and
- Adequately separate the responsibility for making changes to computer programs from the responsibility for installing the changes.

To ensure that its computer resources are adequately safeguarded, the OSP should take the following actions:

- Prevent unauthorized access to its computer systems by individuals from other agencies outside the OSP;
- Require that all critical programs that allow access to the OSP's computer systems be protected from unauthorized access through the use of passwords or some other control measures;
- Restrict access to its computer room to those employees with compatible duties; and

- Require users to sign on to the computer systems with a user identification or password at those terminals that can affect critical data or systems.

To strengthen the documentation of its computer systems, the OSP should take the following actions:

- Provide the minimum documentation necessary for an understanding of processes for those computer systems that will be replaced in the near future; and
- Follow its standards for documenting existing and new computer systems to include complete operation, program, and user documentation.

**Agency
Comments**

The Department of General Services (DGS) stated that, in most cases, the department and OSP are taking action to address the report's recommendations. The DGS also stated that the OSP is assessing the risk associated with lack of password protection at certain computer terminals and is studying the feasibility of adding additional security measures to prevent unauthorized access to its computer system from another state data center.

Introduction

The Office of State Printing (OSP), which is one of 22 offices in the Department of General Services, is mandated by the Government Code, Section 14850, to perform all state printing with some exceptions. It provides printing services for the executive, legislative, and judicial branches of state government, the state university and colleges, and other state agencies in accordance with guidelines established by the State Administrative Manual, Section 2803. Legislative work alone comprises 15 percent of the workload. Printing services range from printing products such as rubber stamps and business cards to printing texts such as the governor's budget and textbooks. The OSP is funded by charges to the agencies served. Annual sales exceed \$50 million.

The OSP has its own on-site electronic data processing (EDP) department, which employed approximately 34 people as of July 1990. It provides data processing services to all of the OSP's departments as well as other state agencies. It consists of six units: Systems Software, Applications, Computer Operations, Special Projects, Customer Liaison, and Word Processing.

- The Systems Software Unit maintains the computer programs that control access to and operation of all the computer systems. Collectively, these programs are called the systems software;

- The Applications Unit performs programming tasks and systems analysis work for the various applications or computer systems. Applications software is designed to accomplish specific functions. For example, a payroll application is designed to process only payroll transactions;
- The Computer Operations Unit operates the computer hardware and peripherals and performs various technical functions. Computer hardware consists of the physical computer equipment, and peripherals are equipment attached to the computer such as printers and disk drives;
- The Special Projects Unit prepares feasibility study reports and acquires, maintains, and installs EDP equipment;
- The Customer Liaison Unit provides assistance to agency customers of the OSP; and
- The Word Processing Unit provides all word processing services and clerical services for the EDP department and other departments at the OSP.

The EDP department also supports the information needs of the OSP's major operations--estimating, production control, material control, accounting, and payroll. For example, the estimating system allows estimators to enter job information through a series of data input screens. The system ultimately produces an estimate of time and cost for a print job. Similarly, the production control system generates production schedules, monitors the progress of jobs as they proceed through the printing plant, and creates management reports describing work performance and job status. Likewise, the stock inventory system uses an on-line terminal system to authorize, issue, and control the OSP's inventory of materials used in the production of the State's many publications. Finally, the accounting and payroll systems provide job accounting information to accounting personnel. The payroll system also provides payroll information to the State Controller's Office.

In addition, the EDP department supports the legislative publication process by transmitting publication files from the Legislative Council Bureau to the OSP to be composed and printed. This process consists of converting computerized coded text of legislative bills and histories, and assembly and senate daily files into text that is printed and used by the Legislature in the bill process.

From April 1989 through March 1990, the EDP department's automated systems helped the OSP to process and control more than 1,000 print jobs per month. Moreover, the stock inventory system provides an up-to-date status of items in the inventory. A current inventory record is essential to ensure that sufficient stock is available and that overstocking and obsolescence does not occur. Because the efficient operation of the OSP is so dependent on computer systems, the systems must be secure and well-managed.

As of February 1991, the EDP department's computer system hardware consisted of an IBM 4341 Model 2 central processing unit (CPU). Attached to the CPU are IBM 3380 disk drives and IBM 3420 tape drives and approximately 60 terminals. The operating system software consists of the IBM MVS operating system. The on-line portion of the computer system is supported by IBM CICS software, Version 1.6, which IBM no longer produces.

Scope and Methodology

The purpose of our audit was to determine the adequacy of the general and application controls over the EDP department. General controls are applicable to all data processing and computer systems within a computer facility. By contrast, application controls relate to individual computerized systems, for example, programmed controls for verifying customer account numbers and credit limits. We accomplished our audit objective by reviewing the EDP department's practices regarding its environmental control, risk management, physical and logical security, computer program changes, and computer system documentation.

To determine whether the environment of the OSP's computer room was adequately protected, we inspected the computer room for potential threats from water flooding, fire, and electrical problems. In addition, we reviewed the backup procedures and inspected the off-site storage of critical computer system files and information databases. Also, we evaluated the OSP's assessment of risk to its computer facility. Additionally, we reviewed the OSP's operational recovery plan and determined the OSP's compliance with standards set forth in the State Administrative Manual, Section 4840, regarding security and risk management.

To determine the OSP's protection over the computer room, terminals, and information databases from damage, theft, and unauthorized entry, we reviewed the OSP's physical and logical security controls used to detect and prevent such problems. Logical security controls usually consist of methods such as user identification codes and passwords to restrict access while physical security controls regulate an individual's movement within a building.

To determine whether changes to computer programs are authorized, tested, and approved, we reviewed the EDP department's procedures for making changes to computer programs and tested program changes to assess the OSP's compliance with the procedures. Moreover, to determine whether the EDP department has adequately documented its computer systems, we compared the documentation of four computer applications with standards for computer system documentation.

**Chapter 1 The Office of State Printing Needs
To Strengthen Its Disaster Recovery Planning
at Its Electronic Data Processing Department**

Chapter Summary The computer systems of the Office of State Printing (OSP) are important assets, ones that must be protected and safeguarded against disaster if they are to consistently operate to service the information needs of the OSP. The first step to protecting these assets is to identify the risks to them to determine where they are vulnerable. Once the risks are analyzed, management has the necessary information to make intelligent decisions about the selection of cost-effective security measures. However, the OSP has not taken adequate measures to detect and prevent floods in the computer room. In addition, the OSP's operational recovery plan did not contain sufficient procedures to effect a recovery following a disaster, nor did it contain plans for an alternate processing site if the computer room became inoperable.

Background Risk management, as defined in the State Administrative Manual, Section 4840.4, is "the process of taking actions to avoid risk or reduce risk to acceptable levels." A risk analysis is used to evaluate and document the risks to an entity, to define the potential impact or cost of losses, and to determine ways to remove or limit risks. For instance, risks to a computer facility may include fires, floods, electrical disturbances, and losses due to accidental and deliberate acts by employees and outsiders. To determine the potential impact or cost of losses, risk analysts would have to determine the cost to replace part or all of the computer facility, the cost to recover or recreate critical information, and the cost of lost productivity. Analysts should also determine an estimate of the probability of an undesirable event occurring. Together, these elements form the basis for

identifying the costs or impact of potential losses. Analysts would then determine ways to remove or limit the risks and the costs of these measures. For instance, water detectors in computer facilities have limited the risk that flooding could occur and go undetected. Analysts must then decide whether the benefits derived from implementing those measures outweigh the costs or impact of potential losses.

Moreover, as part of risk management, an agency should have an operational recovery plan for its computer facility. Although the underlying hope is that the operational recovery plan will never be called on, the risks of not being prepared are too great to ignore. The plan should describe the procedures the agency would use to resume operations following a disaster affecting the facility and should name the person responsible for these procedures.

**Environmental
Security
Needs
Improvement**

Section 4842.2 of the State Administrative Manual recommends that agencies prevent, detect, and minimize water damage and loss or disruption of operational capabilities due to electrical power fluctuations or failure. We believe agencies should install hazard detection devices such as water detectors in their computer facilities and have adequate drainage systems under the floors. Such devices would reduce risk of damage caused by water. However, the OSP's computer room does not have a water detector that would detect water under the floors.

The OSP's computer room also is inadequately protected in other ways against damage caused by flooding. To determine whether the OSP's computer room was protected from the hazards of floods, fires, and loss of electrical power, we inspected the physical location of the computer room in relation to water pipes, fire extinguishers, and electrical boxes and wires. According to OSP staff, during two rain storms in 1989, flooding occurred under the floor of the computer room. Although the subfloor accumulated rain water, no damage was detected. However, if the water had come in contact with electrical boxes and wires, it could have presented a serious threat to employee safety and to the computer room.

The building engineer believed that the two floods were caused by water backing up and not flowing through a drain outlet. The backed up drain outlet caused water to reach the computer room through the computer room's own drainpipe, which is connected to the drain outlet. He remedied this problem by plugging the drainpipe, which is under the floor of the computer room, to keep water from backing up through this pipe. He also installed a pump to handle the condensation runoff from the air conditioning unit. However, plugging the drainpipe leaves nowhere for other water or fluids to flow out of the computer room should such fluids enter it through other means. Thus, we believe closing off the drainpipe presents another hazardous situation.

Specifically, without a way for water or other fluids to drain from the computer room, they could accumulate in the subfloor and cause an electrical shortage. Fluids from the adjacent film development room could potentially flow under the floor of the computer room if the development room's drain system overflowed or backed up. Further, overhead sprinkler pipes in the computer room contain water that could spill out if a rupture or accidental discharge were to occur. Moreover, the air conditioner is located in the computer room and contains chilled water that has the potential to flood the subfloor if a leak were to occur. Although the OSP does have a small pump to remove air conditioner condensation liquid and an alarm system attached to the pump, during our inspection, we tested the pump alarm, and it failed to operate. Therefore, the OSP computer room is inadequately protected against damages due to flooding.

**The
Operational
Recovery
Plan Needs
Improvement**

State agencies are required to prepare an operational recovery plan to respond to disastrous events that could damage and disrupt their computer facilities. According to the State Administrative Manual, Section 4843.1, the operational recovery plan should identify an agency's strategy for managing a disaster, the management and staff responsible for tasks, the computer systems essential to the agency, and the operational procedures that will achieve recovery.

We reviewed the OSP's operational recovery plan and found that it lacked detailed recovery procedures or instructions that could be used by a recovery team to restore operations. (The OSP prepared its plan using the Department of General Services' Operational Recovery Guide.) However, an industry guide for preparing disaster recovery plans and the Stephen P. Teale Data Center recovery plan, which we used as an example of a fully developed plan, included detailed recovery team duties. We believe the OSP's recovery plan could be improved through detailed instructions for the OSP's recovery team members. Although the OSP's plan identified the disaster recovery team manager as having primary responsibility for carrying out the plan and indicated the steps he would have to take to notify computer users if a disaster occurred, the plan did not indicate what procedures other recovery personnel should follow.

In addition, the following important computer systems were not included in the plan: the payroll system, the stock inventory system, the accounting system, and the production control system. We determined that if the payroll system could not operate, timekeeping information would not be as current. Moreover, according to the OSP, if the stock inventory system could not operate for more than a few weeks, the OSP would not be able to control inventory as efficiently and effectively. Also, according to the state printer, if the accounting system and production control system could not operate, the OSP would have untimely data. By not identifying these systems and having procedures in place, the OSP may not be adequately prepared to restore services to its critical systems in the event of a disaster. The only critical system the plan identified was the estimating system, which allows estimators to enter job information to produce cost and time estimates for print jobs.

Also, the plan did not identify an alternative processing site that could be used to provide temporary backup for the OSP's systems in case a disaster made the OSP's computer room inoperable. Without a planned backup site, the OSP may not recover from a disaster without a substantial delay in its critical processing. However, we determined the OSP could obtain a

backup site for processing through an arrangement with the Stephen P. Teale Data Center (Teale). Teale provides backup site services to several state agencies including the Public Employees' Retirement System and the State Compensation Insurance Fund. Teale officials stated that they believe they can meet the computer system requirements of the OSP.

Conclusion We identified weaknesses in environmental security in the computer room of the Office of State Printing. Specifically, we found that the computer room was inadequately protected against damage caused by flooding. We also found that the disaster recovery plan lacked detailed procedures that would facilitate a recovery from a disaster. Finally, we found that the plan did not identify an alternate processing site that could be used to provide temporary backup for the OSP's systems in case a disaster made the computer room inoperable. As a result of these weaknesses, the OSP's computer room may be more susceptible to an extended disruption to processing if a disaster occurs.

Recommendations To improve its ability to recover from a disaster, the Office of State Printing should take the following actions:

- Ensure that water or other fluids can be detected and removed from the computer room and its subfloor;
- Develop procedures in the operational recovery plan detailed enough to ensure the efficient recovery of critical computer systems should a disaster occur; and
- Consider using the Stephen P. Teale Data Center or another facility as a backup site for computer processing in case the computer room becomes inoperable.

Chapter 2 The Office of State Printing Needs To Strengthen Controls Over Changes to Its Computer Programs

Chapter Summary

For most computer systems, programmers must periodically make changes to improve or correct computer programs. These changes to the programs should be controlled through a structured process. Controlling changes made to computer programs is necessary to ensure that they are authorized, designed, documented, and implemented as intended by the requestor of the change, usually the user or data processing management. If program changes are uncontrolled, there is less assurance that the computer systems will function correctly, increasing the risk of invalid management information.

However, the Office of State Printing (OSP) does not always follow a structured process when making program changes. For example, we found program changes that were made without any request documents showing that the changes had been requested, authorized, tested, or implemented. In addition, we found one instance where the changed version of the program was left unprotected and susceptible to further changes of either an accidental or intentional nature. Moreover, we noted that the OSP has not adequately separated the responsibilities for making changes to computer programs and for installing those changes. When the OSP fails to separate duties, it is susceptible to unauthorized changes being made without detection.

Background

Changes to computer programs should be controlled through a structured process to ensure that they are authorized, designed, documented, and tested. These changes should be initiated with

a request from the user, management, or electronic data processing (EDP) staff. Generally, EDP departments use a request document that typically describes the change, the reason for the change, the required implementation date, and the name of the requestor. Before a change is initiated, the appropriate approval should be obtained from the management of the user system and EDP management through a signature on the request document.

When authorization for a change has been given and the computer programmer is ready to make the change to a program, a change control coordinator who is independent of programming may move a working copy of the program into a test library so that the programmer can begin to make the needed change. (Those programs that are actually being used in the daily operations of an agency are run from the production library. Those programs that are undergoing development and testing are run from the test library and should not be used in daily operations.) Before the change development is complete, the programmer must test and document the program. Finally, when changes have been tested and approved and the requestor has accepted them, the changed programs are moved back to the production library by the change control coordinator. Figure 1 illustrates the program change control process as it should be carried out.

**Missing
Change
Requests
for Program
Changes**

Some computer programs perform tasks specific to a business need while others control access to and operation of the entire computer system. The first kind of program we call an individual production program; the second kind, we call a system software program. To determine if only authorized changes were being made to the OSP's computer programs, we sampled 39 changes made to individual production programs and 19 changes made to system software programs. In 13 of the 39 changes to individual production programs and in all 19 of the changes to system software programs, changes were not supported by change request documents. Without these documents, the OSP has no evidence that the changes were requested, authorized, tested, and approved. Unauthorized changes to individual programs could result in errors being inadvertently included in the system or, in the extreme, fraudulent activities committed without timely detection. Moreover, because system software program changes can affect the entire computer system environment, undocumented and potentially unauthorized changes could result in a risk to system integrity. Also, undocumented system program changes can unnecessarily complicate the ongoing maintenance of the computer system. Some examples of changes that were made to system software programs were changes to add or delete terminals, to add or delete data files, and to grant access to users.

We believe that the reason that 9 of the 39 changes were not supported by change request documents was that the OSP considered them minor changes to the programs. However, even minor changes should be adequately supported by documentation. The other 4 of the 13 undocumented changes were initiated by a programmer who did not follow the normal change control procedures. This programmer was able to circumvent the normal procedures because he also is the change control coordinator.

The system software specialist stated that the OSP does not use any internal procedures to document changes to the systems software. He further stated that everyone knows when his group is working on changes and, thus, no documentation is prepared.

Changed Programs Left Unprotected and Susceptible to Further Changes

All authorized, final versions of programs should be executed from the production library. This ensures that the proper version of programs are being used to process data. However, we found that, for eight months, the OSP has been running one program from the test library rather than from the production library. Executing programs from the test library means these programs can be subject to uncontrolled changes by programmers in the process of making other changes to programs for future needs. The program should have been transferred to and run from the production library to ensure greater control over the program.

The program was not moved from the test library to the production library because of an oversight by EDP management, who did not follow change control procedures.

In addition to one program not being moved from the test library to the production library, we found two instances where source codes were exposed to uncontrolled changes by programmers. Computer programs are developed in programming languages known as source code. Computer programmers usually write the programs in source code and then translate or compile the source code into a language understandable to the computer, known as object code. The source code and its translated object code are then stored in the production library for processing.

In the two instances, we found the object code without its corresponding source code because the change control coordinator failed to move the source code at the time the object code was moved into the production library. Storing the source code in the test library creates a risk to the OSP because, while it is in the test library, the source code can be subject to uncontrolled changes by programmers. If the source code were changed, there would be no existing source code version of the program being run unless there is a current backup. The change control coordinator is responsible for moving both source and object code into the production library after the programmer finishes testing and the user and EDP management have approved the program changes.

Failure To Separate Duties in the Change Management Process

The guidelines and auditing standards of the American Institute of Certified Public Accountants and the EDP Auditors Foundation call for complete segregation of duties in the change management process for computer systems. However, the OSP has not adequately separated the responsibilities for making the changes to computer programs (programmer duties) and installing these changes in the production library (change coordinator duties). Specifically, the person that is the change control coordinator at the OSP is also the programmer responsible for making changes to the payroll system. Thus, the change control coordinator has the ability to make changes to payroll production programs and install those changes in the production library. Because the change control coordinator can make changes as well as install them, the change control coordinator could make unauthorized changes without timely detection. If unauthorized changes are made to production systems, recordkeeping errors, incorrect management information, and opportunities for fraud could result.

The change control coordinator is allowed to perform both responsibilities because he is closely supervised; however, supervision does not mitigate the control weakness of the lack of separation of duties. For example, the change control coordinator could change a program to increase someone's work hours and install the change without the supervisor detecting his or her actions.

Conclusion

The Office of State Printing needs to strengthen controls over its changes to computer programs. We found program changes that were made without any request documents showing that the changes had been requested, authorized, tested, or implemented. In addition, we found instances where the changed versions of source codes were left unprotected and susceptible to further changes of either an accidental or intentional nature. Moreover, we noted that the OSP has not adequately separated the responsibilities for making changes to payroll computer programs and for installing those changes. Because the OSP failed to separate duties, it is susceptible to unauthorized changes being made without detection.

Recommendations To strengthen the program change process, the Office of State Printing should take the following actions:

- Ensure that all program changes are documented to show they are requested, approved, tested, and authorized for implementation before they are accepted into production;
- Ensure that all program changes are transferred from the testing environment to the production environment in a controlled fashion so that programs are not left unprotected; and
- Ensure that the employee responsible for installing program changes is not also responsible for making them.

Chapter 3 The Office of State Printing Needs To Strengthen Security Over Its Electronic Data Processing Resources

Chapter Summary

Security controls are the protective measures that are used by an electronic data processing (EDP) facility to reduce the possibility of loss, disruption, or harm to computer programs, information databases, and computer equipment. Security controls protect EDP resources through a combination of access controls, administrative procedures and policies, and software and hardware controls.

Contrary to State Administrative Manual requirements and some of its own policies, the Office of State Printing (OSP) has inadequate security controls over its computer programs, information databases, and computer equipment. Specifically, the OSP has inadequate security controls to regulate access to its computer systems by unauthorized individuals from other agencies outside the OSP. As a result, the OSP could not detect unauthorized attempts to access its systems. Also, the OSP does not require adequate accountability from users of its computer systems. Specifically, the OSP did not password protect critical programs that allow access to and operation of its computer systems. In addition, we found that two software products in use at the OSP inadvertently allow programmers the authority to change computer programs and information databases without approval. Furthermore, the OSP has not restricted access to its computer room to those employees with compatible duties. Finally, we found that nearly everyone in the OSP is allowed to access the computer system through terminals without a user identification or password. Some of these terminals allow users to add or alter data in various applications. As a result of these weaknesses, the OSP has increased its vulnerability to inappropriate program changes, disclosure of sensitive data, and misuse of its computer systems.

Background The State Administrative Manual, Sections 4840 and 4841, provides guidance to state agencies concerning the security controls over sensitive information and information processing facilities and equipment. The OSP's EDP department processes sensitive information and information essential to the ongoing business needs of the OSP; therefore, it is important for the OSP to safeguard this information.

Security controls are necessary to prevent and detect unauthorized access to or use of computer systems. Most computer systems are secured from unauthorized access through the use of logical and physical access controls. Logical access controls consist of identifying all users to a system through a user identification code (user ID) and password. Once the system identifies a user, the user ID is also there to identify every task or job performed by that user, which results in accountability for the user's actions. Moreover, audit trails depend on user ID to track attempts to change programs and databases. Without user ID and password controls, computer systems are susceptible to unauthorized access and usage.

Physical access controls are used to regulate an individual's movement within a building. For instance, the OSP should have security procedures that control access to its computer room because the OSP's computer room contains the EDP equipment for running the OSP's computer programs.

Moreover, separation of duties among individuals is another organizational control that protects an organization from individuals perpetrating errors or irregularities. For instance, as we discuss in Chapter 2, unless other safeguards are provided, such as separating the responsibilities of authorizing, writing, modifying, and operating computer programs among individuals, a programmer could perpetrate fraud by changing program instructions.

The OSP Has Inadequate Controls Over Access to Its Computer From Outside Users

The OSP has inadequate security controls to regulate access to its computer systems by individuals from other agencies outside the OSP. The OSP computer systems are part of a network of interconnected computers that include computers at two state data centers, all of which allow users to transfer data files between computer sites. For example, this computer network is normally used by agencies to transfer and receive data files that are used by the OSP to produce printed material. This is how the Legislature sends its daily agenda file to the OSP to be printed.

During our review, we found that the OSP had no security measures to prevent unauthorized access to the OSP's computer systems by outsiders who could gain such unauthorized access through the state data centers. As a result, the OSP's files and information databases are vulnerable to unauthorized disclosure and, therefore, could be accidentally or intentionally changed or destroyed.

We verified that files could be transferred without authorization or detection between the OSP and the state data centers by users with access to the state data center. From one state data center, we were able to direct the OSP computer to send a copy of an OSP system file from the OSP to the state data center. We then confirmed that the file could be edited and returned to the OSP. In addition, other critical files could have been transferred as well. A security threat to the OSP exists when someone with access to any state data center can gain unauthorized entry into the OSP's computer system.

The OSP Did Not Password Protect Critical Programs That Allow Access to the Entire Computer System

System software programs control the access to and operation of an entire computer system. We believe that effective EDP control practices dictate that the EDP department ensure that such system software programs be protected from unauthorized use or alteration, because access to such programs gives someone access to anything anywhere in the system.

We reviewed the OSP's control over access to these programs and found that programmers are capable of accessing the programs, which are not password protected, and making

unauthorized changes in the security system. Thus, the programmers could gain access to programs or databases they would not normally be allowed to have access to. For example, programmers could access the employee personnel file that contains confidential information about every OSP employee. Because the OSP's system software programs are susceptible to unauthorized changes, its security system, programs, and data files could be compromised and fraud could result.

**The EDP
Department
Has Not
Properly
Controlled
Programmers'
Access
to Computer
Programs and
Databases**

Effective access controls dictate that access to programs and databases be formally controlled to preserve the integrity of the programs and databases. However, the EDP department has allowed programmers the power to modify computer programs and databases without approval. We reviewed the capabilities of two software products in use at the OSP and found that they can give their programmers exceptional authority to modify programs and databases outside the normal change control process.

The authority to modify or delete programs and databases as opposed to only reading them is determined by the computer system through instructions entered by the EDP department. The OSP computer systems granted the highest authority to modify or delete programs and databases to programmers when using one of the software tools. The EDP department's system software specialist installed one of the software tools, known as Switch. Switch was programmed to access a higher security authority than the programmers should have been allowed. Also, according to the state printer, the other software tool, McKinley Systems Online File Utility (OLFU), was given to programmers to make modifications to databases when corrections were needed. However, we found no controls over the use of OLFU. As a result, programmers could make changes without approval or immediate detection.

As a result of these control weaknesses, the OSP has been vulnerable to unauthorized changes to its programs and databases. For instance, to receive additional payments, programmers could

potentially modify the hours in the timecard file. Also, a potentially disgruntled programmer could cause considerable damage to programs and databases. Despite these control weaknesses, we did not uncover any unauthorized activity.

Corrective Action Taken

Before the release of our report, the EDP department took significant steps to correct the problem of programmer access to computer programs and databases. The EDP department instituted an access control procedure over the use of the software tool McKinley Systems Online File Utility (OLFU), which formerly gave programmers exceptional authority to modify programs and databases outside the normal change control process. This new procedure limits programmer access to OLFU and puts control of changes when using OLFU under the responsibility of the manager of the applications unit.

The OSP Has Not Restricted Access to the Computer Room to Those Employees With Compatible Duties

Effective internal controls in EDP departments dictate that there should be a separation between the programming group and the operations group. An application software unit generally designs, writes, and tests computer programs that are turned over to an operations unit after the programs have been approved by management. In contrast, the operations unit operates the computer and the programs authorized by management and maintains the libraries that contain the programs and databases. If the programming unit is not independent of the operations unit, unauthorized modifications are more likely to be made to programs and databases. For instance, programmers are usually aware of the formulas and calculations that are included in programs. If given the opportunity to operate the computer or have physical access to the databases, these employees would have more opportunity to make unauthorized changes to programs and databases. In contrast, operators are not likely to know enough about the design of programs and databases to make changes to them.

To determine whether the OSP was adequately separating the duties of the programming unit and operations unit, we determined whether the OSP was controlling access to its computer room. We reviewed the list of employees who were allowed access. The operations unit has access to the computer room with the exception of the key data entry employees who work outside of the computer room. With certain exceptions, generally the programming unit does not have this access. However, two employees on the list had permanent access even though their duties should have restricted their access. The duties of the two employees consisted of application programming and key data entry into the system. Programming and key data entry duties are considered incompatible with computer room access.

Programs and data files could be more susceptible to unauthorized and undetected changes if employees who have the ability to make changes to computer programs or data files are allowed in the computer room where the programs are operated. This is analogous to the separation of duties in an accounting operation. For instance, effective internal controls require that employees who have access to assets such as cash receipts do not also maintain the accounting records.

**Limited
Accountability
Over Users
of the OSP
Computer
System**

Effective internal controls suggest that all users identify themselves to a computer system with a user identification (user ID) or password to ensure that the individual is authorized to access the system and that the computer system can provide the means to trace all activities to a specific individual. However, we found that, with the exception of EDP department staff who require a user ID and password to use certain technical software in the computer system, computer system users in the OSP are allowed to access the computer systems through terminals without a user ID or password. Some of these terminals allow users to add or alter data in various applications. Allowing users to access the systems without user IDs or passwords creates a risk that unauthorized access or use of the systems could occur.

OSP management uses methods other than user IDs and passwords to restrict access. Restricting terminal access is accomplished through computer security software. For example, through this software, one terminal may have access only to timekeeping programs while another terminal can be prevented by the security software from having that same access. The security software controls access by assigning a number to each terminal. The number determines what abilities a particular terminal has. However, controlling the terminal capability alone does not provide accountability over the actions of individuals. Accountability is improved when computer systems control individual users of the system with a user ID so that any actions may be traced to an individual. Without user IDs, users, without being detected, could initiate unauthorized transactions by simply sitting down and operating a terminal that is authorized to access sensitive programs and databases.

Conclusion

The Office of State Printing has inadequate security controls over its computer programs, information databases, and computer equipment. Specifically, the OSP has inadequate security controls to regulate access to its computer systems by unauthorized individuals from other agencies outside the OSP. As a result, the OSP could not detect unauthorized attempts to access its systems. In addition, the OSP does not require adequate accountability from users of its computer systems. Specifically, the OSP did not password protect critical programs that allow access to and operation of its computer systems. Moreover, the OSP has not restricted access to its computer room to those employees with compatible duties. Finally, we found that nearly everyone in the OSP is allowed to access the computer systems through terminals without a user identification or password. Some of these terminals allow users to add or alter data in various applications. Such weaknesses could lead to unauthorized modifications to programs and information for personal gain.

Recommendations

To ensure that its computer resources are adequately safeguarded, the Office of State Printing should take the following actions:

- Prevent unauthorized access to its computer systems by individuals using the computers at the state data centers;
- Require that all critical programs that allow access to the OSP's computer systems be protected from unauthorized access through the use of passwords or some other control measures;
- Adhere to its policy of not allowing programmers and others with incompatible duties to enter the computer room; and
- Establish an audit trail of users of the computer systems by requiring users to sign on to the systems with a user identification or password at those terminals that can affect critical data or systems.

management, and outside auditors. Also, the OSP requires its EDP staff to follow its own structured development process for documenting computer systems.

Documentation of a computer system should cover three areas: operations, programming, and user. Operations documentation provides operations personnel with the instructions necessary for running the computer system and related applications. Programming documentation describes the computer programs in detail and includes file descriptions and other information for programmers responsible for maintaining the system. User documentation includes a general description of the system and instructions on using the system.

**Weak
Documentation
for Three
of the OSP's
Major Systems**

To determine whether computer system documentation was adequate, we selected four of the eight major computer application systems at the OSP. The four systems were stock inventory, project estimating, accounting, and payroll. For three of the four systems we reviewed, the documentation that was available did not provide sufficient information about the systems for programmers or users to be able to understand them.

In the stock inventory system, we did not find descriptions of 21 programs or descriptions of the reports that these programs produce. Because of this incomplete documentation, it is very difficult to determine how the programs process information or interact and what reports should be received from this system. Minimum documentation for each program should include the following: descriptions of the program; flowcharts or program design specifications; descriptions of how data is formatted for entry into and out of the system; detailed descriptions of file formats and data elements and the elements' position within a file; and records of program changes.

Likewise, many of the programs in the project estimating system were not documented. Without such documentation, it is difficult for programmers to make changes to a program in the system because they cannot be certain how the changes might affect other programs in the system.

Similarly, the accounting system did not have adequate user documentation or program documentation. We interviewed the programmers and nontechnical users of the accounting system and observed a general lack of understanding of system processes. Specifically, we observed that programmers could not explain to us the purpose or function of many system processes contained in flowcharts, and the flowcharts were not explained by any corresponding narratives. Also, for the 32 months from July 1987 through February 1990, system generated information concerning labor costs did not agree with the labor costs reportedly paid. The differences cannot be traced because users do not understand the processes that create the information. Because the differences cannot be traced, the OSP may be using incorrect data from the accounting system to establish labor rates. The users' and programmers' lack of understanding of system processes was caused by not having complete, up-to-date documentation of the system and its programs. According to the manager of the EDP department, the accounting system may be replaced with a new system in the near future.

Lastly, we reviewed the payroll system and found reasonably sufficient documentation from which to understand the system. The documentation included operation procedures, program documentation, detailed process descriptions, and descriptions of the format and content of reports produced by the system.

Conclusion

The Office of State Printing has not adequately documented all of its computer systems. In our review of four of the OSP's eight systems, we found documentation was incomplete or nonexistent for three systems. Undocumented or poorly documented computer systems put programmers and nontechnical users at a disadvantage in maintaining and understanding those systems. Some information from these systems may be unreliable.

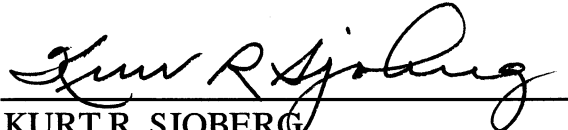
Recommendations

To strengthen the documentation of its computer systems, the Office of State Printing should take the following actions:

- In the short term, provide the minimum documentation necessary for an understanding of processes for those computer systems that will be replaced in the near future; and
- Follow its standards for documenting existing computer systems and new computer systems to include complete operation, program, and user documentation.

We conducted this review under the authority vested in the auditor general by Section 10500 et seq. of the California Government Code and according to generally accepted governmental auditing standards. We limited our review to those areas specified in the audit scope section of this report.

Respectfully submitted,



KURT R. SJOBERG
Auditor General (acting)

Date: July 22, 1991

Staff: Harold L. Turner, Deputy Auditor General,
CDP, CISA
Dennis C. Lloyd, CIA, CISA
Michael C. Dendorfer, CPA, CISA
Diana L. Oretsky
Max Bushman, CPA
Bart R. Thompson

Memorandum

To: Kurt R. Sjoberg
Acting Auditor General
660 J Street, Suite 300
Sacramento, CA 95814

Date: July 12, 1991

From: Office of the Secretary
(916) 323-9493
ATSS473-9493

Subject: RESPONSE TO AUDITOR GENERAL REPORT NO. T-973

Thank you for the opportunity to respond to your Report T-973 entitled "The Office of the State Printing Plant Needs To Strengthen Controls Over Its Electronic Data Processing Resources." The attached response from the Department of General Services addresses each of your recommendations.

If you need further information or assistance on this issue, you may wish to have your staff contact John Lockwood, Director, Department of General Services, at 445-3441.

Best regards,

Barbara Fitzgerald
for BONNIE GUITON
Secretary of the Agency

BG:mb

cc: John Lockwood, Director
Department of General Services

Rick Gillam, Audit Manager
Department of General Services

MEMORANDUM

Date: July 11, 1991

File No: T-973

To: Dr. Bonnie Guiton, Secretary
State and Consumer Services Agency
915 Capitol Mall, Room 200
Sacramento, CA 95814

From: **Executive Office**
Department of General Services

Subject: **RESPONSE TO AUDITOR GENERAL REPORT NO. T-973 -- THE OFFICE OF STATE PRINTING
NEEDS TO STRENGTHEN CONTROLS OVER ITS ELECTRONIC DATA PROCESSING RESOURCES**

Thank you for the opportunity to respond to Office of the Auditor General (OAG) Report No. T-973 which addresses recommendations to the Department of General Services' (DGS), Office of State Printing (OSP). The following response addresses each of the recommendations.

OVERVIEW OF REPORT

The DGS has reviewed the findings, conclusions, and recommendations presented in Report No. T-973. As discussed in this response, the DGS will take appropriate actions to address the recommendations.

Overall, the report presents issues that in most cases OSP management were aware of but had determined that the existing level of risk was acceptable. However, as shown by the following response, the OSP recognizes the concerns of the OAG and, where feasible, is taking action to address the report's recommendations.

The following response only addresses the recommendations. Since they have been extensively discussed in past meetings with OAG staff and in prior correspondence, our disagreements with some specific findings and, especially, the effects and conclusions resulting from those findings, will not be repeated in this response.

CHAPTER 1**THE OFFICE OF STATE PRINTING NEEDS TO
STRENGTHEN ITS DISASTER RECOVERY PLANNING AT
ITS ELECTRONIC DATA PROCESSING DEPARTMENT**

RECOMMENDATION: "Ensure that water or other fluids can be detected and removed from the computer room and its subfloor."

DGS RESPONSE: OSP has included a system for water detection as part of a new security package that is being developed. Installation is anticipated for completion by January 1992.

RECOMMENDATION: "Develop procedures in the operational recovery plan detailed enough to ensure the efficient recovery of critical computer systems should a disaster occur."

DGS RESPONSE: As noted in the report, OSP prepared its plan in accordance with DGS' policies. The area for improvement related to providing detailed team member instructions in operational recovery plans is being studied by appropriate departmental personnel. If deemed necessary, additional guidelines will be provided to DGS' offices.

In addition, OSP considers the estimating system to be the only critical system in operation at the plant. All other systems are subordinate to this primary program. However, OSP does plan to refine the current recovery plan to include the subordinate programs.

RECOMMENDATION: "Consider using the Stephen P. Teale Data Center or another facility as a backup site for computer processing in case the computer room becomes inoperable."

DGS RESPONSE: Teale Data Center (TDC) has been identified as a possible "Hot Site" to provide recovery computer processing. A study due to be completed in December 1991 is being performed to determine if this possibility is cost-effective for the OSP. Also, TDC processing is being considered as an alternative in the Feasibility Study Report for the Fully Integrated System that is currently in the planning stage.

CHAPTER 2

THE OFFICE OF STATE PRINTING NEEDS TO STRENGTHEN CONTROLS OVER CHANGES TO ITS COMPUTER PROGRAMS

RECOMMENDATION: "Ensure that all program changes are documented to show they were requested, approved, tested, and authorized before a change is accepted into production."

DGS RESPONSE: OSP is reviewing its current procedures and a structured method will be implemented for this process. This review is scheduled for completion by September 1991.

RECOMMENDATION: "Ensure that all program changes are transferred from the testing environment to the production environment in a controlled fashion so that programs are not left unprotected."

DGS RESPONSE: OSP is refining its process to ensure compliance with already existing policies.

RECOMMENDATION: "Ensure that the employee responsible for installing program changes is not also responsible for making them."

DGS RESPONSE: OSP is in the process of further defining the responsibilities of the Change Control Coordinator referenced in the report to allow for an improvement in separation of duties. Additional controls should be in place by the end of September 1991. However, it should be noted that the OSP data processing staffing level is small in comparison with large data centers and, by necessity, some duties may overlap.

CHAPTER 3**THE OFFICE OF STATE PRINTING NEEDS TO STRENGTHEN
SECURITY OVER ITS ELECTRONIC DATA PROCESSING RESOURCES**

RECOMMENDATION: "Prevent unauthorized access to its computer system by individuals using the computers at the state data centers."

DGS RESPONSE: Currently, OSP is tied directly only to the TDC and the Legislative Data Center (LDC). OSP has taken action to improve security at TDC by restricting the ability to access OSP files. Specifically, the ability to connect to TDC can only be accomplished by:

- . Direct supervisor authorization, and
- . Must be closed upon completion of the task requested.

This restricts the capability of anyone at TDC having access to OSP's computer. Also, all TDC access is logged by operation.

Preventing unauthorized access at the LDC would be a more difficult process. Specifically, the ability to connect to the LDC is required to ensure the processing of publications such as legislative bills, files and histories transmitted to OSP, a process that can occur at any time throughout the day or night. Limiting this connection would severely jeopardize OSP's ability to serve the needs of the State Legislature. OSP will study the feasibility of adding additional security measures to address the OAG's concerns. However, preliminary conclusions indicate that to achieve the report's recommended level of security would be prohibitively expensive.

RECOMMENDATION: "Require that all critical programs that allow access to the OSP's entire computer system be protected from unauthorized access through the use of passwords or some other control measures."

DGS RESPONSE: OSP is in the process of defining the appropriate methods to control programmer access. However, as previously stated, the programming staff at OSP is small, and, therefore, programmers have overlapping duties. Because of the small number of programmers, any inappropriate changes would be detected fairly quickly by supervisors. However, as much as possible, structured controls will be implemented.

RECOMMENDATION: "Adhere to its policy of not allowing programmers and others with incompatible duties to enter the computer room."

DGS RESPONSE: OSP is studying the feasibility of limiting the access of the two employees referenced in the report.

RECOMMENDATION: "Establish an audit trail of users of the computer system by requiring users to sign on to the system with a user identification or password at those terminals that can affect critical data or systems."

DGS RESPONSE: OSP will perform a risk analysis of the terminals that allow edit updates to determine if user identification or password restrictions are necessary. Currently, where appropriate, OSP has limited terminals by function so that only terminals of appropriate personnel are activated for data input.

CHAPTER 4

THE OFFICE OF STATE PRINTING NEEDS TO BETTER DOCUMENT ITS COMPUTER SYSTEMS

RECOMMENDATION: "In the short term, provide the minimum documentation necessary for an understanding of processes for those computer systems that will be replaced in the near future."

DGS RESPONSE: OSP has an ongoing project to develop documentation for each system. Staff have already developed a comprehensive data dictionary for the Legislative Subscription Service System, and is near completion of one for the Cost Accounting System. Other documentation will be completed as resources are available.

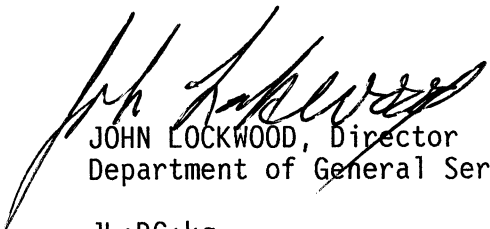
RECOMMENDATION: "Follow its standards for documenting existing computer systems and new computer systems to include complete operation, program, and user documentation."

DGS RESPONSE: Currently, OSP has standards in place for documenting both new systems and revisions to existing systems.

CONCLUSION

As part of its continuing efforts to improve policies and procedures, the DGS will take appropriate actions to address the issues presented in the report. It should be noted that OSP's management has continually shown a strong commitment to improving operations in a timely manner.

If you need further information or assistance on this issue, please call me at 445-3441.



JOHN LOCKWOOD, Director
Department of General Services

JL:RG:kg

**cc: Members of the Legislature
Office of the Governor
Office of the Lieutenant Governor
State Controller
Legislative Analyst
Assembly Office of Research
Senate Office of Research
Assembly Majority/Minority Consultants
Senate Majority/Minority Consultants
Capitol Press Corps**