STATE OF CONNECTICUT

Information System Audit Report

Office Of The State Comptroller

AUDITORS OF PUBLIC ACCOUNTS
KEVIN P. JOHNSTON ❖ ROBERT G. JAEKLE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an audit of the general controls for the Office of the State Comptroller's (OSC) computer operations and reviewed some of the application controls of the Central Accounting System (CAS), during the period of August 7, 2000, through January 29, 2001. The primary objective of this audit was to evaluate the general controls of the Comptroller's information systems in place during this time period. We did obtain and review some of the application controls and gained an understanding of relevant controls for the CAS, but did not audit the application controls.

During our audit work we found some weaknesses in the general controls of the Comptroller's computer operations and other compliance issues that have been identified in the following report. This report consists of an executive summary; the audit objectives, scope and methodology; background information; current audit results and auditee responses; and recommendations. The following is a brief summary of the findings and recommendations from our review.

Physical Security – The physical security of the building housing the Comptroller's computer operations has recently been weakened. Controls need to be implemented to limit the access to the electrical distribution room in this building. A more secure method for distribution of the access code to the data center should be implemented.

Laser Check Stock – The OSC does not perform a count of the boxes of check stock received. Furthermore, the Agency does not maintain a perpetual inventory system for the laser check stock. Check stock was stored in a secure location, but greater inventory control must be maintained to ensure the security of critical documents.

Logical Security – Central Accounting System – We found that some CAS users had different access privileges than what was approved on their Agency or Comptroller On-Line Security Forms. In one instance, we found a user with access privileges that were never approved by the Budget and Financial Analysis Division. In other situations, users had access privileges that were not required or ever used. Security features should be implemented to automatically suspend inactive users after a specified period of time. The minimum required password length is not sufficiently long enough to provide adequate security against password cracking. Users should not be allowed multiple simultaneous log-ins. Agency or Comptroller On-Line Security Forms should be reviewed periodically and access privileges should be tested to ensure that user access privileges are accurate and approved.

Logical Security – Retirement Data Base and Payroll System – User access is not always terminated when employees leave State service. We found nine former employees that

still had valid user identifications codes (Ids) and four other user Ids that appeared to belong to former employees. We were unable to determine if these four Ids belonged to former employees because the OSC did not have adequate documentation on hand to identify the users from other employees with the same name. Agency or Comptroller On-Line Security Forms for the Retirement Data Base were not available for 26 out of 41 individuals reviewed. The OSC should review all active "CM" Logon Ids that have access to the Retirement Data Base System or Payroll System, to ensure that only authorized and active State employees have access.

Software Inventory – The OSC does not maintain a current software inventory that complies with the State of Connecticut's Property Control Manual. Outdated software inventories were identified, but were not complete and did not comply with the State's policy. The Agency should develop and maintain a comprehensive software inventory system.

Business Contingency Plan – The OSC does not have a comprehensive business contingency plan for the Agency's operations. The OSC does have an outdated disaster recovery plan for the mainframe operations, but this plan was not complete or kept current. The OSC does have a contract with a vendor to provide a hot-site disaster recovery facility if a disaster occurred. The OSC does annually perform testing at the vendor's hot site facility. The Comptroller's Office should develop a comprehensive business contingency plan for their operations.

Commitments for Maintenance Agreements – The OSC incurred obligations for maintenance service agreements with two different vendors for the mainframe computer and laser printer, prior to initiating contracts or contract amendments with these vendors. Section 4-98 of the General Statutes requires that agencies enter into a contract with vendors and properly encumber funds prior to incurring obligations. This requirement helps to ensure that funding is available and that the State's interests are protected. The OSC should comply with Section 4-98 of the General Statutes and protect the State's interest with fully executed contracts prior to incurring obligations.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives:

The primary objective of our audit was to evaluate the general controls of the information system administered by the Office of the State Comptroller. Our focus was on the Information System (IS) general controls that effect the CAS. Although our main objective did not include auditing the CAS application controls, we did review and gain an understanding of the significant application controls for CAS.

Scope:

The Auditors of Public Accounts, in accordance with Section 2-90 of the Connecticut General Statutes, are responsible for auditing the books and accounts of all State agencies, institutions supported by the State, all public and quasi-public bodies and other organizations created by public or special act of the General Assembly. Such examinations include the internal control structure of the organizations financial and administrative systems, which include the information systems that State agencies operate or rely upon.

Information System general control audits are examinations of controls which affect the overall organization and operation of the IS function. General controls are the foundation of a secure IS environment and would include the organizational structure, management controls, computer operation, operating system software, logical and physical security, and contingency planning. The effectiveness of general controls has a direct and significant impact on determining the effectiveness of application controls. If general controls are weak or ineffective, application controls may also be rendered ineffective.

Application controls are directly related to specific computer applications. These controls help ensure that transactions are valid, complete, properly authorized, accurately processed and reported. Application controls include programmed control techniques and manual follow-up of computer generated reports.

General and application controls are important elements of the internal control structure and must be effective to help ensure the reliability, confidentiality and the availability of critical information.

Methodology:

Our IS audit was performed in compliance with *General Auditing Standards* issued by the Comptroller General of the United States. Our audit methodology included the following:

- Review of policies and procedures.
- Analysis of applicable reports and any system studies.
- Interviews with key administrators and other personnel.
- Reviews of system manuals and documentation.
- Review of appropriate technical literature.
- Tour of the computer facility.
- On-line testing of system controls.
- Data analysis using audit software tools.
- Review of contractual agreements.
- Review of computer generated reports.
- Observation of computer operations.

Our report was designed to include significant audit results and recommendations developed in response to our audit objectives and report our audit conclusions.

BACKGROUND INFORMATION

The Office of the State Comptroller was formally created in 1786. According to Article Fourth, Section 24 of the State Constitution, "The comptroller shall adjust and settle all public accounts and demands, except grants and orders of the general assembly. He shall prescribe the mode of keeping and rendering all public accounts." In addition to the State Constitution, the Office of the State Comptroller's authority is provided for in Title 3, Chapter 34 of the General Statutes. Such statutes charge the Comptroller to establish and maintain the accounts of the State government; adjust and settle all demands against the State not first adjusted and settled by the General Assembly; to prepare all accounting statements related to the financial condition of the State; to pay all wages and salaries of State employees; to develop, implement and maintain a comprehensive retirement database system and a state-wide time and attendance system; and to administer miscellaneous appropriations for employee taxes, health services and insurance, as well as grants to police, firefighters and municipalities; administer the State Employees Retirement System , Municipal Retirement System and various other miscellaneous retirement systems.

The Office of the State Comptroller employs over 250 staff members and consists of seven divisions that have been assigned various operational responsibilities. These divisions include: Accounts Payable Division; Budget and Financial Analysis Division; Information Technology Division; Management Services Division; Payroll Services Division; Policy Services Division; and Retirement and Benefit Services Division. A significant organizational change that occurred during the 1990's included the distribution of computer programming resources from a central service group to being distributed within the functional divisions. Our review of the Agency's computer operation focused mainly on the Information Technology Division, Central Accounts Payable Division and the Budget and Financial Analysis Division (which includes the former Central Accounting Division).

CAS was developed during the 1980's and has remained relatively unchanged with the exception of some modifications and enhancements to the system. CAS resides on a mainframe computer that is operated by the Agency. It wasn't until the early 1990's that the second phase of the system implementation occurred, this phase was named CAS II and was never widely accepted. By the time that CAS II was implemented, a significant number of agencies had already started using the State Agency Appropriation Accounting System (SAAAS), which is presently administered by the Department of Information Technology.

CAS initially had limited interfaces with other computer systems and data entry was performed centrally. The initial plan was that all State agencies would have terminals connected to CAS and would enter information directly, which was what CAS II was intended to accomplish. By the time that CAS II was implemented, systems such as SAAAS and other agency developed in-house systems had already been adopted and there was a reluctance to convert to CAS II. These other systems provided agencies with the functionality that CAS was intended to provide. The Comptroller decided to allow other accounting systems, such as SAAAS, to interface with CAS which streamlined the data entry effort of State agency personnel and reduced the volume of documents that required data entry by the OSC. Interfaces with other systems have become a significant portion of the transactions that the Comptroller

processes. The majority of agencies process their transactions electronically to CAS through other systems.

The volume of transactions being electronically transmitted increased further with the implementation of the paperless processing and decentralization of document storage initiative. Public Act 93-285 amended Section 3-25, 3-117, 4-37 and 4-98 of the General Statutes, which allowed the State Comptroller to develop and enter into agreements with State agencies for the retention of accounting information at each State agency. These statutory revisions allowed the Comptroller to initiate the paperless processing effort, which has streamlined the accounting and expenditure processing.

Over the years, State agencies have been purchasing and implementing new information systems without considering the implications of providing interfaces with other existing State systems. The lack of a unified objective and focus has left the State with a significant number of different systems operating on different types of technologies, that don't always communicate with each other smoothly. The lack of a central focus for the State has created a complicated web of core systems and various interfaces for these systems. Adding to this complicated web of systems, a number of core financial systems have become antiquated and are in need of replacement.

Currently, the State of Connecticut is engaged in the process of replacing and consolidating the State's core financial systems, which will include the State Accounting, Payroll, Personnel and Human Resources systems. Other modules for the core system may include inventory tracking, budgeting and possibly a new retirement system. The new system will use Enterprise Resource Planning software that will integrate the State's core financial systems and should eliminate the need for redundant systems. This initiative is a joint effort between the Office of the State Comptroller, the Department of Administrative Services, the Department of Information Technology and the Office of Policy and Management. Significant cooperation from other State agencies has and will continue to be needed for this initiative to be successful.

AUDIT RESULTS AND AUDITEE RESPONSES

Item No. 1. Physical Security

The physical security of the building housing the Comptroller's Office was weakened when changes were enacted to the contract with the security vendor for the building. These changes may not be immediately apparent to the occupants of the building but have significantly weakened the overall security of the facility. Surveillance of the Data Center should be improved when the data center is unoccupied. The building security system already has key pieces of security elements that can readily be used to enhance the overall security of the building without substantial capital outlay.

Access to the electrical distribution room should be controlled to restrict unauthorized entry and to ensure the safety of the employees. Personnel from other State agencies need access to the electrical distribution room to reach storage facilities that can only be accessed through this room, but the building management firm and a limited number of agency personnel should be the only individuals having access to this room. Unauthorized individuals accessing the electrical distribution room could potentially cause a disruption of services to the entire building and pose a safety hazard.

The access code to the Comptroller's Data Center is periodically changed to provide improved security. We found that the access code for the Data Center was not distributed in a secure manner. Although it appeared that no security breaches have occurred, changes should be implemented to provide greater control over the distribution of the access code for the Data Center.

Physical security of the building housing the CAS should be improved and access should be restricted to the electrical distribution room. Distribution of access codes should be performed using a secure method. (See Recommendation 1.)

Agency Response:

"The Information Technology Division of the Office of State Comptroller (ITD/OSC) has reviewed the auditor's recommendation and is revising its method of access code distribution to secure the Data Center. Effective immediately, the Operations Manager will notify authorized personnel by e-mail that the access code is being changed. Those authorized personnel will then have to see the Operations Manager or Supervisor in person to obtain the code, which will be verbally communicated."

"Regarding access to the electrical distribution room, building management has been notified of our concern and has taken the necessary steps to secure the room at all times."

Item No. 2. Laser Check Stock

The Comptroller's Office upgraded the check printing process during the 1999-2000 fiscal year and converted from impact printed checks to laser printed checks. This change involved defining new requirements for laser check stock that provide appropriate security features. Using the laser printer to produce vendor, payroll and retirement checks has significant advantages over the previous check stock because more information is printed at the OSC. These changes will allow the Comptroller's Office to quickly adapt to changes in elected officials or bank account information, which previously has been a significant expense to the State. The new check stock no longer has preprinted check numbers, but does have sequence numbers printed on the backside for control purposes. Converting the check printing process to the laser printer provided a significant reduction in the time required for the printing process.

We found that controls over the laser check stock were weak because of the lack of inventory control of the check stock stored at the OSC. The laser checks are delivered to the Comptroller's Office on pallets with approximately 50 cartons per pallet and each pallet is shrink wrapped. The number of pallets received can vary depending on how many checks the agency requests. Each delivery is reviewed for reasonableness but the actual cartons are not counted. The OSC staff retains the packing slip that lists the number of boxes and check stock control numbers. The OSC does not maintain a perpetual inventory of the number of laser checks received and currently controlled by the Agency. We noted that a control log was maintained to record and verify the first and last check used for each run. The check stock is stored in a secure location, but physical counts of the total number of cartons received and a complete perpetual inventory should be maintained for the laser check stock.

The OSC should physically count all cartons of laser check stock when received and maintain perpetual inventory records to account for laser check stock on hand. Periodically, physical inventory counts should be performed to verify the perpetual inventory. (See Recommendation 2.)

Agency Response:

"Based upon the recommendation of the auditors, ITD/OSC has developed an improved method for inventorying and tracking check stock. Upon delivery, agency staff will account for all cartons before signing off on packing slips. Any cartons of check stock moved from the storage area will be noted on a perpetual inventory log. The operations supervisor will regularly verify this log. The contents of each individual carton and ream are currently verified by the operator before use, including the preprinted inventory control numbers."

Item No. 3. Logical Security – Central Accounting System

Our review of 25 users with access to the CAS revealed that ten individuals' access to the CAS was different from the approved access indicated on their Agency or Comptroller On-Line Security Form. These forms are used to request a user Id and password for access to the CAS and document the approval of these requests. In addition, we found one individual with access to CAS that was not approved by the Budget and Financial Analysis Division, and the CAS access rights requested on their Agency or Comptroller On-Line Security Form were different from their actual access rights.

Our review of the separation of duties among the CAS rights revealed that nine users had the ability to audit release expenditures, transfers and maintain transfer documents. Two users had the ability to audit release commitments, transfers and maintain transfer documents. All 11 of the users were not approved by the Agency to have these access capabilities.

We found that four CAS users out of 25 did not use or need some or all of their CAS access rights. Access rights for all CAS users should be periodically reviewed and users that do not need or use their access to the CAS should have their access rights revoked. Controls should be established and defaults should be set to suspend a user's Id when that user does not access the CAS for a specified period of time.

We noted that passwords needed to access the CAS should be lengthened for improved security. Users can access the CAS from multiple locations at the same time, which should not be allowed for all users. Information system staff may need the ability to access CAS from multiple locations at the same time, which may be acceptable in limited situations.

The OSC should initiate a review of all CAS user Ids for accuracy of such access rights and to verify the users' continuing need for this access. The OSC should review and modify password policies to strengthen security. (See Recommendation 3.)

Agency Response:

"ITD/OSC will require that all CAS users resubmit their user ID forms so that an accurate master list of users can be developed. Division directors will be asked to periodically review the access levels for their employees, and the master list will be changed accordingly. Any changes will be immediately placed into the system."

"ITD/OSC is currently reviewing its password design structure and will take further action to improve security. The unit is also evaluating user ability to access CAS from multiple locations at the same time, and will be having discussions with division directors regarding the need for this flexibility vis a vis security of the system."

Item No. 4. Logical Security – Retirement Data Base and Payroll System

Our review of 41 individuals with assigned "CM" Logon Identification Codes (Ids) to access the agency Retirement Data Base System revealed that eight individuals were no longer active State employees. One individual with an assigned "CM" Logon Id to access the agency Payroll System and/or the Retirement Data Base System is not an active State employee.

We were unable to determine for four out of the 41 individuals reviewed if these individuals were active State employees, due to the agency not having adequate documentation on hand to identify the users from other State employees with the same or similar names.

We found that for 26 out of the 41 individuals reviewed, there were no Agency or Comptroller On-Line Security Forms on hand with the OSC. These forms are used to document that an individual is authorized to have a "CM" Logon Id to access the Retirement System.

A review of all employees with active "CM" Logon Ids that have access to the Retirement Data Base System or Payroll System should be completed to ensure that only authorized and active State employees have access. (See Recommendation 4.)

Agency Response:

"ITD/OSC is currently reviewing its records of active "CM" Logon Ids. All employees with inappropriate access or those who have left state service will be purged from access to the system. On a regular basis, ITD/OSC will review CATER's quarterly list of authorized users in conjunction with OSC personnel records to ensure accuracy of the authorized user list. ITD/OSC will also confirm CATER's guidelines for automatic deletion of inactive Ids."

Item No. 5. Software Inventory

The OSC does not maintain a current centralized or decentralized comprehensive software inventory. The State of Connecticut's Property Control Manual requires that agencies maintain a software inventory and produce annual reports that shall be available to the Auditors of Public Accounts. Without a software inventory being maintained, the OSC can not be sure that they are in compliance with the State of Connecticut's Software Management Policy Manual.

The Information Technology Division provided us with a centralized software inventory list dated August 13, 1999. This list did not contain the required minimum data elements prescribed by the State of Connecticut's Property Control Manual. We were informed that this list did not contain all of the software installed on the Agency's Personal Computers (PCs). We were

informed that in addition to this list, the Agency completed a scan in 1999 of PCs using a software program to generate a data file of software installed on their PCs. This software list does not constitute a software inventory, but could be used for the development of such an inventory. We were also informed that the software for the mainframe computer was not on the inventory listing.

Upon our request, the Comptroller's Office used a software program to produce a report of software installed on the OSC's file servers. The report that was generated did not contain the required minimum data prescribed by the State of Connecticut's Property Control Manual. The report did not specify the number of licenses that the OSC owns for any network software. Monitoring the usage of software provided on the local area network (LAN) should be performed for software packages, which the Agency owns fewer copies of than the total number of users.

We inquired of the Agency's Divisions to determine if decentralized software inventories were maintained. One Division provided us with a current list of software that it acquired, which was not provided via the OSC LAN. This list did not contain the required minimum data prescribed by the State of Connecticut's Property Control Manual. Other divisions did not maintain software inventory listings.

The OSC should develop and maintain a comprehensive software inventory system. (See Recommendation 5.)

Agency Response:

"In order to comply with the State of Connecticut Software Management Policy Manual, ITD/OSC will take the following actions:

- *Conduct software scans of all primary and secondary agency servers as well as all desktops in order to produce an inventory of installed software.*
- *Perform a physical inventory to obtain license agreements (and/or copies of purchase orders) for installed software.*
- *Institute an inventory control process upon receipt of newly purchased software. This system will contain all information necessary for compliance with the software management policy.*
- *Perform quarterly scans of desktops and servers to maintain accurate inventory records."*

Item No. 6. Business Contingency Plan

Inquiries of Agency staff determined that the OSC did not have a formal Business Contingency Plan in place that covered the organization's entire operation. The OSC had a disaster recovery plan from 1995 and a partial plan from 1997 that together made up the Agency's disaster recovery plan. These two documents together were not all encompassing and did not include all of the required contacts. These documents were also outdated and included contacts that no longer worked for the Comptroller's Office. Copies of the most recent disaster recovery plan were not widely distributed and a copy of the plan was not stored off-site. Agency personnel should be aware of the disaster recovery plan and understand their individual roles in carrying out this plan.

We noted that the OSC has a formal schedule for backing-up critical data and for the storage of such data off-site. We also noted that the OSC has a contract in place with a vendor to provide the Agency with disaster recovery telecommunications and hot-site services. The OSC performs annual tests of the telecommunication and hot-site services. However, a current and complete Business Contingency Plan to restore the Agency's services and to repair or reconstruct its Data Center in the event of a disaster has not been established.

The contract between the Comptroller's Office and their disaster recovery service provider specified that the vendor would annually have an independent audit of their operations performed and provide the OSC with a copy of this report. The OSC has not received or reviewed copies of the audit reports of their disaster recovery vendor's operation.

A formal written Business Contingency Plan that covers all of the Comptroller's operations and the permanent recovery of such operations should be completed and approved by an authorized individual. Individuals involved with implementing the plan should receive periodic training in the use of the emergency procedures covered by the plan. A copy of the Business Contingency Plan should be kept in relevant off-site storage.

The OSC should ensure that annually it receives and reviews a copy of an audit report of the hot-site vendor's operations. (See Recommendation 6.)

Agency Response:

"ITD/OSC is currently in the process of developing a Business Contingency Plan. Phase I includes the OSC Local Area Network, the Central Accounting System (CAS), and the Accounts Payable System. This phase is expected to be completed by September 2001. Phase II of the BCP will address those systems currently processed at the DOIT Data Center. The completion of Phase II is contingent upon the development of a disaster recovery plan for those systems by DOIT staff, as well as upon the status of the CORE-CT project, which will be replacing those systems. An Emergency Procedures Manual is also being written, a copy of which will be secured at the OSC's off-site storage facility."

" ITD/OSC management has taken steps to ensure that the agency receives the required annual audit report from the hotsite vendor."

Item No. 7. Commitments for Maintenance Agreements

We obtained copies of contracts that the OSC entered into for maintenance of its mainframe computer and laser printer to ensure that the information systems were being properly maintained. In reviewing these contracts, we noted the contract periods started prior to the date the contracts were signed and implemented. Section 4-98 of the General Statutes requires that no budgeted State agency shall incur an obligation without a valid commitment document in place.

We noted that the OSC incurred obligations of $18,189 for a maintenance agreement for computer hardware and software prior to the execution of a purchase order. In another instance, the Agency allowed a maintenance agreement for their laser printer to expire twice, prior to initiating a contract amendment. With regard to the maintenance agreement for the laser printer, the Agency incurred obligations totaling approximately $14,000 without a valid commitment in place.

Obligating the State without having a contractual agreement in place could result in the failure to receive the expected services. Non-compliance with statutory requirements could result in the OSC exceeding its appropriation.

The OSC should comply with Section 4-98 of the General Statutes and protect the State's interest with fully executed contracts prior to incurring obligations. (See Recommendation 7.)

Agency Response:

"ITD/OSC will in the future make sure that all contract procedures are in full compliance with Section 4-98 of the General Statutes."

RECOMMENDATIONS

1. **Physical security of the building housing the CAS should be improved and access should be restricted to the electrical distribution room. Distribution of access codes should be performed using a secure method.**

   Comments:

   Changes to the physical security contract have occurred recently that have weakened the overall security of the building. Access to some areas of the building should be restricted to improve the overall security of the information systems and the general safety of the employees. Periodic changes to access codes should be distributed by means of a more secure method than is currently being used.

2. **The OSC should physically count all cartons of laser check stock when received and maintain perpetual inventory records to account for laser check stock on hand. Periodically, physical inventory counts should be performed to verify the perpetual inventory.**

   Comments:

   Our review noted that cartons of check stock are not counted when they are delivered and that perpetual inventory records are not maintained for the check stock. We noted that a control log was maintained to record and verify the first and last check used for each run.

3. **The OSC should initiate a review of all CAS user Ids for accuracy of such access rights and to verify the users continuing need for this access. The OSC should review and modify password policies to strengthen security.**

   Comments:

   A review of all employees with CAS user Ids should be completed to ensure that users are only allowed to access options that they need to perform their job duties and that have been approved. Individuals no longer requiring some or all of their access capabilities to the CAS should have their access modified or revoked. Controls should be put into place or defaults should be set to suspend a user's Id if the user does not access the CAS for a specified period of time. Security controls should be implemented

to prevent users from being able to access the CAS from multiple locations at the same time. The agency should increase the required length of the user passwords for the CAS.

4. **A review of all employees with active "CM" Logon Ids that have access to the Retirement Data Base System or Payroll System should be completed to ensure that only authorized and active State employees have access.**

   Comments:

   Employees' no longer requiring access to the Retirement Data Base System or Payroll System should have their access promptly revoked. Appropriate procedures should be implemented to provide for a systematic process to ensure that access to information systems is terminated promptly.

   Agency or Comptroller Online Security Forms identifying all authorized users of the agency Retirement Data Base System should be maintained by the OSC.

5. **The OSC should develop and maintain a comprehensive software inventory system.**

   Comments:

   We noted that the OSC does not currently maintain a comprehensive software inventory system. Incomplete and outdated software inventory records were provided that did not comply with the State of Connecticut's Property Control Manual. Furthermore to avoid software-licensing violations, monitoring of software installed on the Comptroller's LAN should be performed for any shared software package that the Agency owns fewer copies of than total users.

6. **A formal written Business Contingency Plan that covers all of the Comptroller's operations and the permanent recovery of such operations should be completed and approved by an authorized individual. Individuals involved with implementing the plan should receive periodic training in the use of the emergency procedures covered by the plan. A copy of the Business Contingency Plan should be kept in relevant off-site storage.**

   The OSC should ensure that annually it receives and reviews a copy of an audit report of the hot-site vendor's operations.

Comments:

The OSC had a disaster recovery plan that covered the information systems mainframe. The plan was not currently updated and was not widely distributed. The OSC has a formal schedule for backing-up critical data and for storing such data off-site. We also noted that the OSC has a contract in place with a vendor to provide disaster recovery telecommunication and hot-site services.

7. The OSC should comply with Section 4-98 of the General Statutes and protect the State's interest with fully executed contracts prior to incurring obligations.

Comments:

During our review of the maintenance agreements for the Comptroller's mainframe computer and laser printer, we noted that the agency had incurred obligations with two vendors prior to initiating contracts or contract amendments with these vendors.

CONCLUSION

In conclusion, we wish to express our appreciation of the courtesies shown to our representatives during the course of the audit. The assistance and cooperation extended to them by the Office of State Comptroller in making their records readily available and in explaining the control environment greatly facilitated the conduct of this examination.

Bruce C. Vaughan
Principal Auditor

Approved:

Kevin P. Johnston
Auditor of Public Accounts

Robert G. Jaekle
Auditor of Public Accounts

1202-IS-01