STATE OF CONNECTICUT

CORE-CT

General Controls Audit Report

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 Core-CT Financial and Human Resource Management System (HRMS), through March 2007. The Core-CT system is the State of Connecticut's central Financial and Human Resource Management System. The primary objective of this audit was to evaluate the general controls of the agency's information systems in place during this time period. We did not review the application controls for the Core-CT system. We will perform separate application controls audits for the Core-CT Financial and HRMS systems.

During our audit work we found some weaknesses in the general controls of the Core-CT system 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.

Password Security – Our review of the Core-CT system's security revealed that improvements over user passwords could be improved by implementing existing security features that are available in the software. Access security for the Core-CT system should be reviewed and modifications should be made to comply with the State of Connecticut's Information Security Policy.

Active User Accounts – Our review disclosed that, out of a randomly generated sample of thirty user IDs, there were three instances where employees separated from State service and their user IDs had remained active. In a separate test of four terminated employees, we found that all four user IDs had remained active after the associated users had separated from State service. The Core-CT security administration group should develop procedures to ensure that a periodic review of each agency's user IDs is conducted and any unnecessary user accounts are deactivated in a timely manner.

Security Badges – We found that security badges that grant access to the building housing the Core-CT operations were not always returned when employees terminated. One security badge assigned to an individual who separated from State service remained active after his/her termination date. Additionally, the security badges for two employees that had terminated were used subsequent to each individual's termination date. Core-CT staff should promptly collect ID badges from all State employees or contractors who no longer require access to the building. A periodic review of all access IDs for Core-CT staff and contractors should be conducted to ensure that only necessary IDs remain active.

Service Level Agreement – We were informed that no service level agreement exists between the Core-CT project and the Department of Information Technology (DOIT) covering the services provided by DOIT's data center. A written service-level agreement detailing the responsibilities of the Core-CT Project team and DOIT should be developed and implemented.

Disaster Recovery Plan – Our review disclosed that a comprehensive disaster recovery plan that has been completely and thoroughly tested does not exist for the Core-CT system. We also noted that no agreement exists outlining the responsibilities of the Core-CT management and the Department of Information Technology in the event of a disaster. A comprehensive disaster recovery plan for the Core-CT system should be developed and completely tested. The Core-CT management and the Department of Information Technology should draft a memorandum of understanding to identify each entity's responsibility in the event of a disaster.

Steering Committee Meetings – We were informed that the Steering Committee had not formally met from June 9, 2004, through the third quarter of 2005. We were also informed that meeting minutes do not exist for any Steering Committee meetings that may have been held. The Steering Committee should resume meetings immediately in order to be in compliance with the terms of the memorandum of understanding. The minutes of the meetings held should be properly documented.

Core-CT Policy Board – Our review of the Core-CT project disclosed that the Policy Board, which should have been established pursuant to Section 3-115d of the General Statutes, has not met as required by subsection (b) of this Section. The Core-CT Policy Board should meet quarterly in order to comply with Section 3-115d, subsection (b), of the General Statutes.

Background Checks – We determined that from the four agencies; Department of Administrative Services, Office of Policy and Management, Office of the State Comptroller and the Department of Information Technology, that are responsible for the Core-CT project, three of the four agencies do not perform any background checks on newly hired employees. Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT project.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives:

The primary objective of our audit was to evaluate the general controls of the Core-CT information system. Our focus was on the Information System (IS) general controls that affect the CORE-CT system. Our objective did not include auditing the Core-CT application controls; we will review and gain an understanding of the application controls for Core-CT in two separate subsequent audits.

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.

IS 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 *Government 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 is designed to include significant audit results and recommendations developed in response to our audit objectives and to report our audit conclusions.

BACKGROUND INFORMATION

Core-CT is the system that has replaced Connecticut State government's core financial and administrative computer systems including central and agency accounting, purchasing, accounts payable, payroll, time and attendance, personnel, inventory and asset management systems.

Prior to the implementation of Core-CT, the State of Connecticut was operating numerous systems on different platforms, written in a number of different languages. This situation created a difficult environment for integrating information and lead to redundant data entry and wasted resources performing reconciliations between the various systems. In addition, the systems were administered by different agencies with different priorities.

The State's central administrative agencies - the Office of the State Comptroller (OSC), the Department of Administrative Services (DAS), the Department of Information Technology (DOIT) and the Office of Policy and Management (OPM) banded together to undertake the transition to a new, integrated system encompassing virtually all major administrative functions and all executive-branch State agencies. The system uses enterprise resource planning (ERP) software to tie together all functions, using an integrated suite of software applications, common databases, and a unified technical architecture.

The State contracted with Accenture to assist with the evaluation and selection process prior to the State choosing the PeopleSoft software applications for Core-CT. The State then decided to contract with Accenture for consulting services to assist with the implementation of the PeopleSoft applications. Currently, Accenture continues to be employed by the State to provide assistance with the implementation and upgrades of the Core-CT system.

The Core-CT system implementation included the use of PeopleSoft Financials, Enterprise Performance Management (EPM) Ad-Hoc Reporting, and the Human Resource Management System (HRMS) software. PeopleSoft Financials (Phase I), EPM and HRMS were implemented into production during July 2003, September 2003 and October 2003, respectively. The Core-CT financials Phase I implementation included the general ledger, purchasing, accounts payable and accounts receivable modules. The Core-CT financials Phase II implementation occurred during 2005 and included the billing, assets, and inventory modules. The projects and contracts modules are scheduled to be implemented during 2007. HRMS includes modules for payroll, time and labor, human resources, and benefits. The EPM ad-hoc reporting function allows users to query on the data warehouse and produce custom reports.

Since the initial implementation of Core-CT, the HRMS application was upgraded from version 8.3 to version 8.9 in May 2006, and the Financials application was upgraded from version 8.4 to version 8.9 in November 2006.

PeopleSoft Corporation was taken over by Oracle during January 2005. Oracle has publicly committed to supporting the PeopleSoft software applications until at least 2013.

Core-CT Steering Committee:

- Nancy Wyman, State Comptroller
- Robert Genuario, OPM Secretary
- Anne Gnazzo, DAS Commissioner
- Diane Wallace, Chief Information Officer (DOIT)

Core-CT Project Directors:

- Jim Shumway, OSC
- Gale Mattison, OPM
- Cathy Daly, DAS
- Jeanne Skellett, DOIT

Below is a brief description of the four agencies that have worked together to create the Core-CT system and the statutory authority that each agency has regarding the system. Each of these agencies has broad authorities that cover many areas that are unrelated to the Core-CT system and therefore we have limited the agency descriptions to Core-CT relevant areas.

The Office of the State Comptroller:

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 agency 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.

Department of Administrative Services:

The Department of Administrative Services (DAS) operates primarily under the provisions of Title 4a, Chapter 57 of the General Statutes. DAS is charged with: (1) The establishment of personnel policy and responsibility for the personnel administration of State employees; (2) The purchase and provision of supplies, materials, equipment and contractual services, as defined in section 4a-50. Other programs prescribed include the administration of the set-aside program (also known as the Supplier Diversity Program), distribution of State and Federal Surplus Property, prequalification of contactors to bid on contracts for the construction, alteration, repair or demolition of public buildings by the State or a municipality. (3) The publishing, printing or purchasing of laws, stationery, forms and reports; (4) The collection of sums due the State for public assistance; (5) State Fleet Operations; (6) The Small Agency Resource Team (SMART) was established, effective July 1, 2005, under Section 60(c) of Public Act 05-251. It required the Commissioner of Administrative Services, in consultation with the Secretary of the Office of Policy and Management, to develop a plan for the Department of Administrative Services to provide personnel, payroll, affirmative action and business office functions for various State agencies. As a result, the personnel, payroll, and affirmative action functions of 22 agencies were subsequently merged and consolidated within the Department of Administrative Services.

Department of Information Technology:

The Department of Information Technology (DOIT) operates under the provisions of Title 4d of Chapter 61 of the General Statutes. The Agency was created by Public Act 97-9 of the June 18, 1997 Special Session of the General Assembly. The legislation that created the Department of Information Technology combined divisions and functions that previously were part of the Department of Administrative Services, Office of Information Technology. DOIT was created to provide statewide guidelines, policies and procedures for the use of information technology by State agencies. DOIT is responsible for the procurement of information and telecommunication systems for executive branch agencies, along with providing services to State agencies through the State Data Center. Section 4d-8 of the General Statutes provides that the Chief Information Officer, under the provisions of Title 4a, shall purchase, lease, and contract for information and telecommunication system facilities, equipment, and services.

Office of Policy and Management:

The Office of Policy and Management (OPM) operates under the provisions of various State Statutes. Primarily, it operates under Title 4, Chapter 50, and Title 16a, Chapters 295 through Chapters 298b, of the General Statutes. The Secretary of OPM is appointed by the Governor. OPM has broad statutory authority as the agency serves as a centralized management and planning agency. As described in Section 4-65a, OPM is responsible “for all aspects of state planning and analysis in the areas of budgeting, management, planning, energy policy determination and evaluation, intergovernmental policy, criminal and juvenile justice planning and program evaluation”.

Pursuant to Section 4-66 of the General Statutes, OPM’s fiscal and program responsibilities include the following:

- To keep on file information concerning the State’s general accounts

- To participate in the making of State capital (physical plant and equipment) plans.
- To convey financial information to the General Assembly and the State Comptroller.
- To review and assist in improving the operations of State agencies.

OPM is also responsible for various oversight and control functions, for instance:

- The preparation and implementation of the State's budget - Chapter 50, Part II (Sections 4-69 to 4-107a) of the General Statutes.
- The establishment of agency financial policies; the review and approval of budgets for financial systems and taking action to remedy deficiencies in such systems; the advising of agencies of financial staff needs; the recommending of career development programs for managers; and the coordination of transfers of financial managers are responsibilities assigned to OPM's Office of Finance under Section 4-70e of the General Statutes.
- The oversight and coordination of contracting by State agencies for outside personal service contractors. Personal service contractors provide consulting or other contractual services to State agencies - Chapter 55a (Section 4-205 through Section 4-229) of the General Statutes.
- The administration of the Capital Equipment Purchase Fund used to purchase capital equipment for State agencies - Section 4a-9 of the General Statutes.
- The Office of Labor Relations (OLR) within OPM acts on behalf of the State in collective bargaining and other roles requiring employer representation. Under the provisions of Chapter 68 ("Collective Bargaining For State Employees") of the General Statutes, the Governor has designated OLR to act as the representative of the State.

AUDIT RESULTS AND AUDITEE RESPONSES

Findings:

Item No. 1 – Password Security

Criteria: The State of Connecticut Information Security Policy and Procedures, dated April 12, 1999, provides that users must choose passwords that are “difficult-to-guess” and “must not be a word found in the dictionary, or some other part of speech.” The Policy also states that, “where such systems software facilities are available, users must be prevented from selecting easily guessed passwords.”

Condition: Our review of the password security controls over Core-CT disclosed that although the ability to prevent users from choosing passwords that are easily guessed exists within the Core-CT system, this feature is not being utilized.

Our review also disclosed that the system has the ability to prohibit the reuse of previous passwords, but this feature is not being utilized.

Effect: The lack of strong security access controls may increase the risk of unauthorized access to the system and possible destruction or the manipulation of system data.

Cause: We were informed that, during the initial implementation of Core-CT, the specificity of password composition (other than length) was not required, nor has this topic since been addressed. The password history feature was not available when the system was implemented and was not activated when it became available.

Recommendation: Access security for the Core-CT system should be reviewed and modifications should be made to comply with the State of Connecticut’s Information Security Policy. (See Recommendation 1.)

Agency Response: “The capability identified in this finding, which prevents users from choosing passwords that are easily guessed, is not a delivered feature in the Password Controls functionality. To address this finding, we plan to review delivered password controls, such as Password Character Requirements. By enabling predetermined character requirements, we can enforce that user passwords include a special character or number, which would ensure that passwords are not an easily guessed word.

The system is delivered with the capability to prevent users from reusing passwords. The Password History Control feature allows us to identify the number of passwords the system will retain to verify that a password is not being reused. We are not currently using this feature, but we plan to evaluate it, identify any limitations and possible implementation issues, and determine how to best apply it."

Item No. 2 – Active User Accounts

Criteria: Pursuant to an email sent to Agency Security Liaisons, dated October 20, 2003, Agency Liaisons are responsible for requesting deletion of access immediately upon the notice of an employee's termination, retirement, or transfer to another State agency.

Condition: Our review disclosed that, out of a randomly generated sample of thirty user IDs, there were three instances where an employee separated from State service and their user ID had remained active. In a separate test, we judgmentally tested four terminated employees and found that all four user IDs had remained active after the associated user had separated from State service.

Effect: The lack of strong logical security controls increases the risk of unauthorized access to the system and possible manipulation or destruction of data.

Cause: Established procedures were not properly followed.

Recommendation: The Core-CT security administration group should develop procedures to ensure that a periodic review of each agency's user IDs is conducted and any unnecessary user accounts are deactivated in a timely manner. (See Recommendation 2.)

Agency Response: "It is the responsibility of each agency, through their Security Liaison, to approve the set-up, modification, and deactivation of user accounts on Core-CT through submission of the proper documentation. The OSC will issue a Comptroller’s Memorandum informing agencies that they must notify the Core-CT Security Team within 24 hours of the termination of an employee who was a Core-CT user so that his or her account can be deactivated.

Further, Core-CT will review reports on a quarterly basis that identify terminated employees who still have active user accounts to identify agencies that are not regularly deactivating accounts as employees leave State service. Agencies will be notified in writing of any problems found.”

Item No. 3 – Security Badges

Criteria: The Department of Information Technology’s (DOIT) security policies dictate that, “Upon termination of employment or services rendered at the DOIT site, it is up to the Director, Manager or Supervisor to collect ID badges and any keys that the person may have had and return them to Facilities Management.”

Condition: One security badge assigned to an individual who separated from State service remained active after his/her termination date. Additionally, the security badges for two employees that had terminated were used subsequent to each individual’s termination date.

Effect: The physical security of the building housing the Core-CT operations is weakened when terminated employees continue to have access to the building. The risk of unauthorized access to the Core-CT offices and the destruction of critical information could occur.

Cause: The access cards were not returned to DOIT’s Facilities Management upon the employees’ separation.

Recommendation: Core-CT staff should follow the Department of Information Technology’s Security Policy and promptly collect ID badges from all State employees or contractors that no longer require access to the building. These badges should be returned to DOIT’s Facilities Management. A periodic review of all access IDs for Core-CT staff and contractors should be conducted to ensure that only necessary IDs remain active. (See Recommendation 3.)

Agency Response: “It is the established practice to retrieve badges from Core-CT employees who leave State service, or from consultants whose contract has ended, on the last day of employment as a part of the separation process. In order to ensure that this is occurring, we will review a list of active ID badges for employees and contractors on a quarterly basis to verify that ID badges are active for only those people who require access to the building.”

Item No. 4 – Service Level Agreement

Criteria: Sound business practices dictate that agreements between two parties should be outlined in written form to ensure the effective performance, from all parties, of the responsibilities stipulated by the agreement.

Condition: We were informed that no service level agreement exists between the Core-CT project and the Department of Information Technology (DOIT) covering the services provided by the DOIT’s data center.

Effect: Without a service level agreement the services provided are not properly defined and the services delivered may be inadequate.

*Cause***:** We were informed that a service level agreement between Core-CT and DOIT was being discussed but was never signed or agreed upon by either party. It could not be determined why the Core-CT project and DOIT have not developed a service level agreement.

Recommendation: A written service-level agreement detailing the responsibilities of the Core-CT Project team and the DOIT should be developed and implemented. (See Recommendation 4.)

Agency Response: “We agree with this recommendation. Core-CT will begin working with DOIT to develop a service level agreement for the services DOIT provides to Core-CT. The scope of this agreement will be the technology services DOIT provides enterprise-wide, as well as to Core-CT, such as network services, job scheduling, data storage, data back-ups, and disaster recovery.”

Item No. 5 - Disaster Recovery Plan

Criteria: Sound business practices provide that organizations have current and comprehensive disaster recovery plans in place to enable the resumption of critical operations within a reasonable period of time after a disaster occurs.

Condition: Our review disclosed that a comprehensive disaster recovery plan that has been completely and thoroughly tested does not exist for the Core-CT system.

We also noted that no agreement exists outlining the responsibilities of the Core-CT management and the Department of Information Technology in the event of a disaster.

Effect: The lack of a comprehensive disaster recovery plan would affect the ability of the State to resume its daily critical business operations in a timely manner.

Without an agreement defining the responsibilities of each party, further delays to the recovery of the Core-CT system in the event of a disaster could occur and may lead to additional costs to the State.

Cause: We were informed that it is the understanding of the Core-CT management that their disaster recovery efforts will be incorporated in the formalized plan being developed by the Department of Information Technology.

We were also informed that all roles and responsibilities will be clearly outlined in a document that the Department of Information Technology is in the process of creating and for which Core-CT management will provide input.

Recommendation: A comprehensive disaster recovery plan for the Core-CT system should be developed and completely tested. The Core-CT management and the Department of Information Technology should draft a memorandum of understanding to identify each entity's responsibility in the event of a disaster. (See Recommendation 5.)

Agency Response: **"**We agree with this recommendation. Historically, DOIT has had the responsibility for providing a disaster recovery program for the systems run at the State Data Center, but for years there was no viable disaster recovery program in place. As early as 1999, the Comptroller raised the issue in writing with DOIT about the lack of a viable disaster recovery program for the OSC's Payroll and Retirement systems. When Core-CT moved into production in 2003, the Comptroller again raised the issue of the lack of a disaster recovery program. It was soon thereafter that DOIT initiated a program through a contract with IBM to test and implement a disaster recovery program for its mainframe-based systems as well as for Core-CT.

The disaster recovery process that DOIT chose, known as "crate and ship", relied on restoring the system and its data from tape at a disaster recovery cold site. The first test of this process took place in August of 2004. Six additional tests were conducted with gradually increasing levels of success, but the Core-CT team concluded that this recovery process would not meet the business needs in terms of acceptable system recovery time and extent of data loss.

Core-CT is now well in to the process of re-architecting and implementing a disaster recovery solution which mitigates both the risk of lost access to the system and its data. These risks will be mitigated by creating a constant, fully replicated copy of our data at a remote disaster recovery site. We expect to have this replicated data copy in place by September 2007. We will continue to coordinate with DOIT's disaster recovery testing to establish a comprehensive, integrated test plan. Operational procedures will be developed as we have done with our previous disaster recovery methodology.

A comprehensive disaster recovery plan is being developed by DOIT with input from Core-CT management. The initial draft is scheduled to be completed for June 30, 2007. It is in this document that all of the roles and responsibilities of the applicable DOIT and Core-CT staff will be outlined."

Item No. 6 - Steering Committee Meetings:

Criteria: Pursuant to the "Memorandum of Understanding [MOU] Among The Office of the State Comptroller, the Department of Information Technology, the Department of Administrative Services, and the Office of Policy and Management Regarding The Replacement Of The State's Core Financial and Administrative Computer Systems" dated August 29, 2000, the Core-CT project shall have an Executive Steering Committee. The Steering Committee shall be made up of the State Comptroller, the Chief Information Officer, the Commissioner of Administrative Services, and the Secretary of OPM, and shall oversee the Core-CT project. The Committee shall make all decisions by unanimous consent. This Committee also has final approval over the procurement authority vested in the Project Directors.

Sound business practice dictates that minutes of meetings should be kept in order to record basic information such as the actions assigned and decisions made.

Condition: We were informed that the Steering Committee had not formally met from June 9, 2004, through the third quarter of 2005.

We were also informed that meeting minutes do not exist for any Steering Committee meetings that may have been held.

Effect: The Steering Committee is not in compliance with the terms of the MOU. The risk that decisions may be made without the unanimous consent of the Committee as well as procurements being made without the proper authority is increased.

Without meeting minutes, an accurate record of actions taken or decisions made does not exist.

Cause: We were informed that meetings are usually initiated by the Steering Committee Chair and that the "Chair may have felt there to be no need for a meeting."

Recommendation: The Steering Committee should resume meetings immediately in order to be in compliance with the terms of the MOU. The minutes of the meetings held should be properly documented. (See Recommendation 6.)

Agency Response: "The Core-CT Steering Committee has met periodically, as necessary, throughout the course of the Core-CT implementation and since the system has been in production. All final decisions regarding vendor selection, software selection, and the implementation scope and schedule have been made by the Steering Committee. The MOU does not dictate how frequently the Committee must meet, so the Committee is not violating the terms of the MOU.

We agree that meeting minutes should be published for all future meetings of the Committee."

Item No. 7 - Core-CT Policy Board:

Criteria: Connecticut General Statute 3-115d provides that, there is established a Core-CT Policy Board which shall meet at least once during each calendar quarter and at such other times as the chairperson deems necessary. The Policy Board's primary responsibility shall be to ensure and maintain the constitutional and statutory independence of the three branches of State government with respect to the implementation and operation of the Core-CT system. In addition, the Policy Board shall establish, implement and oversee interagency and interdepartmental policies, procedures and protocols and enter into written agreements that assure that appropriate controls are in place within the Core-CT system with respect to data access, data sharing and data security

Condition: Our review of the Management Controls relative to the Core-CT project disclosed that the Policy Board, established pursuant to Section 3-115d of the General Statutes, has not met as required by subsection (b) of this Section.

Effect: By the Core-CT Policy Board not meeting, it may not be fulfilling its primary responsibility of ensuring and maintaining the constitutional and statutory independence of the three branches of State government with respect to the implementation and operation of the Core-CT system. In addition, they can not be assured that the appropriate controls are in place within the Core-CT system with respect to data access, data sharing and data security.

Cause: We were informed that, “The establishment of the Core-CT Policy Board was done as the Core-CT system was being implemented in case any issues arose… Since that time there have not been issues raised and therefore the board has not met.”

Recommendation: The Core-CT Policy Board should meet quarterly in order to comply with Section 3-115d, subsection (b), of the General Statutes. The Board should establish interagency and interdepartmental policies, procedures and protocols for Core-CT pursuant to Section CGS 3-115d, subsection (d) of the General Statutes. (See Recommendation 7.)

Agency Response: “This Policy Board was established at the request of the Judicial Branch to address issues related to the security of the information in the system for the three independent branches of government. The board was intended to meet to address issues that could arise during the implementation affecting their operations. The Policy Board did not meet and to-date has not met because problems related to the specific issues the Board was charged with addressing did not arise."

Item No. 8 - Background Checks:

Criteria: Sound business practice dictates that background checks should be performed on all newly hired employees that have access to sensitive or classified data.

Condition: We interviewed personnel from the four agencies; Department of Administrative Services, Office of Policy and Management, Office of the State Comptroller and the Department of Information Technology, responsible for Core-CT and determined that three of the four agencies do not perform any background checks on newly hired employees.

Effect: The Core-CT project personnel have access to sensitive and classified data. If background checks are not completed, this data, as well as the software applications are put at an increased risk of theft, destruction and/or alteration.

Cause: Although a specific cause was not identified, it appears that each agency, with the exception of the Department of Information Technology, did not complete background checks prior to the implementation of Core-CT. In addition, it appears that the lack of a specific agency having clearly defined responsibility and accountability over the Core-CT project increases the confusion over who is responsible for these background checks.

Recommendations: Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT project. (See Recommendation 8.)

Agency Response: "There is no provision that we are aware of that requires that criminal background checks be conducted for administrative employees – employees who are not in public safety, correctional, revenue services, or health care settings."

Auditors' Concluding Comments: Although no legal requirement may exist, sound business practices suggest that background checks should be performed for all employees.

RECOMMENDATIONS

1. **Access security for the Core-CT system should be reviewed and modifications should be made to comply with the State of Connecticut's Information Security Policy.**

   Comments:

   Security features that are included in the Core-CT systems are not currently being utilized. Implementing the password security features would significantly enhance the overall security of the system.

2. **The Core-CT security administration group should develop procedures to ensure that a periodic review of each agency's user IDs is conducted and any unnecessary user accounts are deactivated in a timely manor.**

   Comments:

   We found that some Core-CT user IDs remained active after these users had terminated State service. A periodic review of all active user IDs should occur to ensure that users no longer requiring access to the Core-CT system have their access terminated. Agencies should be required to verify that all of their users still require access to the system.

3. **Core-CT staff should follow the Department of Information Technology's Security Policy and promptly collect ID badges from all State employees or contractors that no longer require access to the building. These badges should be returned to DOIT's Facilities Management. A periodic review of all access IDs for Core-CT staff and contractors should be conducted to ensure that only necessary IDs remain active.**

   Comments:

   We found instances where security badges were not collected and returned to DOIT's Facilities Management. DOIT's security policy specially requires that agency management must collect all security badges from terminated employees and return the badges to DOIT.

4. **A written service-level agreement detailing the responsibilities of the Core-CT Project team and DOIT should be developed and implemented.**

Comments:

No service level agreement exists between the Core-CT Project team and the Department of Information Technology (DOIT) covering the services provided by DOIT's data center.

5. **A comprehensive disaster recovery plan for the Core-CT system should be developed and completely tested. The Core-CT management and the Department of Information Technology should draft a memorandum of understanding to identify each entity's responsibility in the event of a disaster.**

Comments:

Our review disclosed that the Core-CT system does not have a comprehensive disaster recovery plan that has been completely and thoroughly tested.

6. **The Steering Committee should resume meetings immediately in order to be in compliance with the terms of the MOU. The minutes of the meetings held should be properly documented**

Comments:

We found that the Core-CT Steering Committee was not meeting on a periodic basis and that no minutes for their meetings exist.

7. **The Core-CT Policy Board should meet quarterly in order to comply with Section 3-115d, subsection (b), of the General Statutes. The Board should establish interagency and interdepartmental policies, procedures and protocols for Core-CT pursuant to Section 3-115d, subsection (d), of the General Statutes.**

Comments:

We found that the Core-CT Policy Board has never met and has not developed policies or procedures as required by Section 3-115d of the General Statutes.

8. **Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT project.**

Comments:

Given the significant time, effort and financial outlay that the State has invested to develop the Core-CT system and the sensitive nature of the data, background checks should be performed on all employees.

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 employees of the Office of State Comptroller, the Department of Administrative Services, the Office of Policy and Management and the Department of Information Technology 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