STATE OF CONNECTICUT

AUDITORS' REPORT
CORE-CT SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF NOVEMBER 2014

AUDITORS OF PUBLIC ACCOUNTS
JOHN C. GERAGOSIAN ❖ ROBERT M. WARD

Table of Contents

STATE OF CONNECTICUT

AUDITORS OF PUBLIC ACCOUNTS

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

JOHN C. GERAGOSIAN

ROBERT M. WARD

May 7, 2015

AUDITORS' REPORT
CORE-CT SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF NOVEMBER 2014

We have audited certain operations of the Core-CT system in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to, the period ending November 2014. The objectives of our audit were to:

1. Evaluate the system's internal controls over significant management and financial functions;

2. Evaluate the system's compliance with policies and procedures internal to the department or promulgated by other state agencies, as well as certain legal provisions; and

3. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the department, as well as certain external parties; and testing selected transactions. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United

States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

The State Auditors' Findings and Recommendations in the accompanying report presents any findings arising from our audit of the Core-CT system.

COMMENTS

FOREWORD

Core-CT is the name given to Connecticut's integrated Human Resource Management System (HRMS) and Financials system. The Core-CT system was implemented in 2003 to replace numerous older legacy systems to provide standardization, increased ad hoc reporting capabilities, simplified reconciliation, and an interactive user environment. Core-CT is a comprehensive system that includes the State of Connecticut's accounting; purchasing; accounts payable; accounts receivable; project costing; inventory and asset management systems; payroll; benefits; human resources; and time and labor functions.

The Office of the State Comptroller (OSC) and the Department of Administrative Services (DAS) jointly administer and maintain the Core-CT system. The system uses enterprise resource planning (ERP) software to incorporate all business functions, using an integrated suite of software applications, common databases, and a unified technical architecture. In addition to standardized reports, the Core-CT system utilizes an Enterprise Performance Management (EPM) ad-hoc reporting function. The EPM ad-hoc reporting function allows users to query the data warehouse and produce custom reports.

The Core-CT staff is divided into seven functional teams: HRMS, Financials, EPM-Ad-Hoc Reporting, Technical, Security, Level 1 Help Desk, and Organizational Readiness. Descriptions of the major Core-CT functional teams are presented below.

HRMS Team

The HRMS team works to ensure that the modules of Core-CT dealing with HR functions (Human Resources, Payroll, Benefits and Time and Labor) are configured to meet the State of Connecticut's business process needs. The HRMS Team is also responsible for the design, development, testing, and delivery of HR and payroll processing system modifications.

Financials Team

The Financials team works to ensure that the modules of Core-CT supporting Financials processes (Chart of Accounts, Budgeting, General Ledger, Accounts Payable, Purchasing, Asset Management, Inventory, Accounts Receivable/Billing, Project Costing, and Customer Contracts)

are working to meet the State of Connecticut's business process needs. The Financials team is also responsible for the design, development, testing, and delivery of financials system modifications.

EPM-Ad-Hoc Reporting Team

The EPM team is responsible for the design, development, and delivery of an intuitive ad-hoc reporting system for Core-CT. The team administers the statewide data warehouse/information repository that is the technical backbone of the system's advanced enterprise-wide reporting capabilities.

Technical Team

The Technical team is responsible for Core-CT's technology infrastructure. The team manages the selection, configuration and maintenance of the servers, software, and communication network that form the backbone of Core-CT. The Technical team ensures that the various technical components of Core-CT (interfaces, security, batch processing, and reporting) are functioning properly, interfacing correctly per system specifications and business needs, and performing at optimal levels.

Below is a list of the Core-CT Steering Committee and Project Directors, along with a brief description of the two agencies that collaborate to maintain the Core-CT system and the statutory authority that each agency has regarding the system. Each of these agencies has broad authority covering many areas unrelated to the Core-CT system; therefore, we have focused the agency descriptions to relevant areas that affect the Core-CT system.

Core-CT Steering Committee:

- Martha Carlson, OSC Deputy Comptroller
- Martin Anderson, DAS Deputy Commissioner

Core-CT Project Directors:

- Martha Carlson, OSC – Deputy Comptroller
- Martin Anderson, DAS – Deputy Commissioner
- Angelo Romano, OSC – Core-CT Director

The Office of the State Comptroller:

The Office of the State Comptroller operates primarily under the provisions of Article Fourth, Section 24, of the State Constitution and Title 3, and Chapter 34 of the General Statutes. Under the provisions of Section 3-115a of the General Statutes, the Comptroller shall provide for the budgetary and financial reporting needs of the executive branch as may be necessary through the Core-CT system.

In addition to the Core-CT organizational reporting structure, OSC employees on the Core-CT financial team are under the Budget and Financial Analysis Division of OSC and the OSC employees on the Core-CT HRMS team are under the Payroll Services Division of OSC. The Core-CT technical team is under OSC Information Technology Division.

Department of Administrative Services:

The Department of Administrative Services operates primarily under the provisions of Title 4a, Chapter 57 of the General Statutes. Descriptions of the major functions of the department that are relevant to the Core-CT system are presented below.

The department's responsibilities which significantly impact the Core-CT system include: providing statewide human resource services that include the establishment and administration of personnel policies of state employees; the purchase and provision of supplies, materials, equipment and contractual services, as defined in section 4a-51 of the General Statutes; and the purchase and contracting for information systems and telecommunication system facilities, equipment and services for state agencies, as defined in sections 4d-1 and 4d-2 of the General Statutes.

It should be noted that effective July 1, 2011, a significant agency reorganization took place, and DAS absorbed the functions of certain other agencies. Pursuant to Public Act 11-51, all statutory authority of the former Department of Information Technology was transferred to the Department of Administrative Services – Bureau of Enterprise Systems and Technology.

In addition to the Core-CT organizational reporting structure, DAS employees on the Core-CT HRMS team are under the DAS Statewide Human Resources Management Division and DAS employees on the Core-CT Financial team are under the DAS Procurement Services Division.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our review of the controls environment of the Core-CT system revealed certain areas warranting attention that are discussed in the following findings.

Core-CT Login Schedules

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53). Control AC-02 (12), Account Monitoring/Atypical Use, requires that the organization "monitor information system accounts for organization-defined atypical use" and "report atypical usage of information system accounts or organization-defined personnel," and indicates that atypical usage includes, for example, "accessing information systems at certain times of the day…that are not consistent with the normal usage patterns."

Condition: It was the intention of Core-CT to use two roles in the system to restrict the hours of the day in which each user is able to sign on. However, sign-on schedules with 24/7 access were inadvertently assigned to other permission lists that were associated with user default sign-on roles, thereby superseding the role having a permission list restricting most user sign-on times to the hours of 6am to 7pm. As a result, all Core-CT users were able to access the system 24/7 at the time of our testing.

Further testing indicated users were able and did run Core-CT reports at times they were unauthorized to do so.

Effect: Users were able to access Core-CT and use state resources during times in which they were not authorized to do so.

Cause: Core-CT sign-on schedules were not properly configured.

Recommendation: The Core-CT security administration group should take steps to ensure that permission lists are always assigned appropriate sign-on schedules. (See Recommendation 1.)

Agency Response: "All permissions lists that should not have 24/7 access have been corrected. The Security Team is implementing bi-weekly procedures which include several new queries for auditing user access and include instructions on rectifying any security issues promptly. It should be noted that 24/7 access is only restricted to users before 4am and after 8pm to allow for system processing and not because Users are necessarily 'unauthorized' to access the data."

Database (Back-end) Password Controls

Criteria: The National Institute of Standards and Technology recommends various identification and authentication controls (IA) in its special publication 800-53 (SP 800-53). Control number IA-05, Authenticator Management, requires that the organization:

a. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

b. Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];

c. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];

d. Prohibits password reuse for [Assignment: organization-defined number] generations

Core CT's database vendor's official security guide notes, "When you create a user account, the database assigns a default password policy for that user. The password policy defines rules for how the password should be created, such as a minimum number of characters, when it expires, and so on. You can strengthen passwords by using password policies."

Condition: Core-CT's applications utilize four production databases on the back-end. In our review of the password policies enforced by each database, we noted the following:

a. Database users can reuse the same password infinitely.

b. Database users can have the same password throughout the life of their account; they are not prompted to change their password after X days.

c. Database users are not locked out after a set number of failed login attempts, with the exception of one of the four databases. In that database, a user is locked out for seven days after ten failed login attempts. That is the only production database with such a rule.

d. Database users are not bound by any complexity requirements when choosing a password.

Effect: As noted in the application's database security guide, "passwords are vulnerable to theft, forgery, and misuse…" and this lack of strong password controls increases the risk of such vulnerabilities.

Cause: Password policies were not properly configured in the back-end production databases.

Recommendation: The Core-CT security administration group should take steps to ensure that password controls are properly configured in the back-end production databases. (See Recommendation 2.)

Agency Response: "Core-CT agrees with this recommendation. A new user profile for all user ids will be created to enforce: minimum password length and complexity requirements; password lifecycle and password expiration periods; user id locking due to unsuccessful sign on attempts."

Core-CT Segregation of Duties Conflicts

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53). Control AC-05, Separation of Duties, requires that the organization:

a. Separates organization-defined duties of individuals;

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

A strong control system relies upon appropriate segregation of duties among employees so that no one individual can subvert a critical process.

Conflicting Core-CT roles within the Human Resources Management System (HRMS) are defined within the Core-CT HRMS Role Handbook.

Conflicting Core-CT roles within the Financials system are defined within the Core-CT Segregation of Duties Matrix.

Condition: At the time of our review, 265 employees throughout 40 departments had the ability to both create and pay a person within Core-CT. This

collective ability is prohibited by the Core-CT HRMS Role Handbook unless agencies provide written justification along with a description of the compensating controls that the agency has implemented to prevent abuse. As described by the Core-CT HRMS Role Handbook, such conflicting roles "could allow an individual to hire and pay someone inappropriately and without oversight."

Core-CT personnel did not have documentation on file – from the applicable agencies – to support why 81 out of 265 employees (31%) had this combination of roles.

Two employees, one in each of two departments, have conflicting roles in the application's inventory module as defined by the Core-CT Segregation of Duties Matrix governing the application's financials system and its modules.

Core-CT personnel were unable to provide evidence of waivers or exceptions having been granted to these two employees.

Core-CT personnel do not maintain a log of which employees have been granted an exception or waiver to Core-CT policies regarding conflicting roles. Information such as when a waiver is granted, by whom, for whom, for what roles, or for how long, is not recorded or maintained.

Effect: Overlapping roles can have a detrimental effect on internal controls. The risk of impropriety is increased if such roles are not segregated.

Without a log documenting which employees were granted exceptions to specific rules, the ability of Core-CT staff to monitor whether or not rules are followed is severely inhibited.

Cause: Established procedures were not followed. Other causes could not be determined.

Recommendation: Core-CT personnel should strengthen controls over segregation of duties conflicts within the Core-CT system and develop a means of tracking any exceptions or waivers granted to certain employees or departments. (See Recommendation 3.)

Agency Response: "DAS's Core-CT staff has taken numerous steps in recent years to improve Core-CT security and to ensure that only appropriate individuals have the ability to make changes to critical data. A statewide review took place in the fall of 2013 to identify all employees with conflicting roles. Agencies were required to review the security access of those employees to determine whether the need for such roles

remained. If so, agencies were required to re-request the roles and provide updated information as to the need and the procedures in place at the agency to prevent fraud. Requests were submitted for review and approval via the automated CO-1092 Security Request Form implemented in October 2012. Since this process is now automated, all supporting documentation is now electronically stored. All agencies with the exception of one have fully complied in the Executive, Legislative and Judicial Branches. Higher Education continues to work on this issue."

Application Controls re: Confidential Data

Background: Core-CT's applications allow developers to configure both table level and row level security. The applications allow system administrators to configure user access to tables and rows of those tables, based on logical criteria such as business unit, department ID, or other such values.

In addition, column level security restricts designated groups of employees from viewing certain columns of tables. For example, if a column of a table contains confidential information, such as a Social Security number, a view of a table may be created which selects all of a table's data except for columns containing the confidential information. Users without the need for access to the confidential information are only granted access to the restricted view rather than the complete table.

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53). Control AC-06, Least Privilege, requires that the organization "employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Condition: In our review of a highly sensitive table that holds every state employee's full name, residential address, birthdate, and Social Security number (SSN), we found that six employees – who do not work at a central service agency – had access to rows representing employees of at least one department other than their own, despite not having any need for such access.

We also identified five additional employees at a central service agency who do not appear to require access to any HR information, yet each had access, through this table, to the full name, residential address,

birthdate, and SSN, for between 17 and 29 departments in addition to their own.

Effect: Many employees had excessive access to confidential employee information at the time of our testing. It cannot be determined whether this access was abused. The lack of strong controls in this area leaves state employees vulnerable to having their personal information accessed by employees of other departments who have no need to access such information. There is an increased risk that confidential information could be leaked to outside parties.

Cause: Row level security and table level security were not properly implemented.

Recommendation: The Core-CT security administration group should develop procedures to ensure that all database application controls are used where appropriate and configured properly to prevent unauthorized access to confidential information. (See Recommendation 4.)

Agency Response: "User Security in Core-CT was automated in 2013 which includes an approval workflow component where designated OSC and DAS employees can review, approve or deny department, business unit or roles by user in all applications. Provisions for attachments or comments documenting justification for any exceptions are also included. This has helped eliminate many of the errors they may have occurred with the previous manual process. In addition, the Security Team is implementing bi-weekly procedures which include several new queries for auditing user access (row security and query access groups*) and include instructions on rectifying any security issues promptly. It should be noted that table security is only configured in EPM*."

Deactivation of Database Usernames Belonging to Separated Employees and Consultants

Criteria: The National Institute of Standards and Technology recommends various personnel security controls (PS) in its special publication 800-53 (SP 800-53). Control PS-04, Personnel Termination, requires that the organization, "upon termination of individual employment, disables information system access" within an organization-defined time period. It is good business practice to disable access on an employee's last day of work.

Condition: We found that 27 individuals who were previously consultants or separated state employees had access to the database at the time of our testing. While they are unable to login from a location when not

connected to the state network, there is still a risk that they could enter a state office building and connect to the Internet, through which they could then interact with the database using whatever privileges are associated with their username.

In addition, we found that 41 usernames were unaccounted for on the log of usernames maintained by the Office of the State Comptroller and 197 accounts, while recorded on the log, did not identify the employee or consultant associated with the account.

Effect: There is an increased risk of unauthorized access to the Core-CT back-end databases and possible manipulation or destruction of data.

Cause: The cause could not be determined.

Recommendation: The Core-CT security administration group should develop procedures to ensure a periodic review of who has access the databases behind the Core-CT system and ensure that user accounts are deactivated in a timely manner. (See Recommendation 5.)

Agency Response: "Core-CT agrees with this recommendation. Procedures will be established to conduct periodic reviews of Oracle user ids and database level access with the goal of deleting or deactivating unneeded accounts in a timely manner."

Database Privilege Logging and Monitoring

Criteria: The National Institute of Standards and Technology recommends various access controls in its special publication 800-53 (SP 800-53). Control AC-02, Account Management, "requires approvals by organization-defined personnel for requests to create information system accounts," and for each account's access to the information system to be based on "a valid access authorization."

Condition: While formal procedures exist, including the completion of forms, when Core-CT front end access is requested, granted, or modified, there are no such formal, documented procedures covering access to the Core-CT back-end databases.

We found that such access, while limited primarily to select central service agency staff, is typically granted over email and is not logged on any record. While data dictionary views within the database allow you to look at a current snapshot of who has access to what, it cannot be determined, for each user, when the user was granted access or by whom. Although the grantor of the role or privilege is provided, only

the user account is shown, and in the case of some system usernames, it cannot be determined which database administrator executed the grant.

Formal, periodic database security audits, consisting of an examination of what privileges have been assigned to which users – whether directly or indirectly through a role – are not completed by Core-CT staff, neither at the object nor system level.

In addition, we found that 160 user accounts, among the four production databases, have the ability to create a table, specific to their schema, and to grant privileges to other users on those tables in which they personally create. However, these users only appear to require read only access to the database.

Effect: There is an increased risk of unauthorized access to the Core-CT back-end databases and possible manipulation or destruction of data.

Cause: The cause could not be determined.

Recommendation: The Core-CT security administration group should develop procedures to ensure a periodic review of the access each database user has and to ensure that access levels are appropriate and consistent with job duties. (See Recommendation 6.)

Agency Response: "Core-CT agrees with this recommendation. The RESOURCE role will be removed from the production Oracle user accounts. This role is what allows users to create tables in their user schema.

An automated monthly report will be created in each production database: HRPRD, FNPRD, EPPRD, and PEPRD. This report will list the granted roles for each Oracle account. Module leads will be responsible for reviewing the reports to ensure appropriate levels of access are granted, and to identify any accounts that should be removed.

Note: for Core-CT development and functional personnel, select access is granted with the SYSADM_S role. This provides these users with read-only query access to all data tables in the environment. This is appropriate for their PeopleSoft development and functional job duties."

Shared Database Account with Confidential Data Access

Background: Core-CT was implemented in 2003 to replace the state's legacy software applications. As such, Core-CT payroll data only goes back to 2003.

Payroll data prior to 2003 is still at times needed by current state employees in the conduct of their job duties. Such data was brought directly into the Core-CT back-end – behind HRMS – for this reason.

Criteria: The National Institute of Standards and Technology recommends various identification and authentication controls (IA) in its special publication 800-53 (SP 800-53). Control number IA-02, Identification and Authentication, requires that the organization's information system "uniquely identifies and authenticates organizational users."

Condition: We found that multiple employees of the Office of the State Comptroller (OSC) use a single database user account to access historical pay data, which resides in the database behind the HRMS system. The historical pay data from 1990 to 2002 contained an average of 88,478 Social Security numbers per year, in addition to each employee's full name and residential address. The shared account had access to any and all of the rows from these tables.

In addition, the user account that owns these tables also had a password identical to its username at the time of our testing. The OSC employees who were granted view-only access to the tables owned by this other user had the ability to determine the username that owned the tables by accessing data dictionary views within the database. Had any of them done so, and guessed that the password for that username was the same as the username, they would have been able to login as the owner of those tables. By logging in as the table owner, they would have freely been able to delete, modify, or add data to these tables.

Effect: There is an increased risk of unauthorized access to the Core-CT back-end databases and possible manipulation or destruction of data.

Cause: The cause could not be determined.

Recommendation: The Core-CT security administration group should develop procedures to ensure that no single database user account, with the exception of system usernames used by database administrators, is shared by more than one individual, and that passwords never match their associated usernames. (See Recommendation 7.)

Agency Response: "Core-CT agrees with this recommendation. A procedure will be developed to ensure that access to these tables follow the same standards as noted in the "Database (Back-end) Password Controls" finding."

Database Accounts Where Password = Username

Criteria: The National Institute on Standards and Technology Special Publication 800-132, Appendix A, Section 1, states that "For the security of electronically stored data, passwords should be strong enough so that it is infeasible for attackers to gain access by guessing the password."

The Core-CT Security Liaison Guide states that User-IDs and passwords should not be shared for convenience between personnel. While this policy governs the Core-CT front end, it would be good business practice to enforce the same rule on the Core-CT back-end databases.

Condition: We reviewed all user accounts within each database that owned one or more objects to determine whether we could login using the username as the password. We determined that eight accounts had the same password as the username, and we were successfully able to login to these accounts. In doing so, we had the ability, while logged in, to delete, modify, or add data to any and all of the objects owned by these users. Most of these objects were tables holding data related to historical pay, backups of queries, and backups of other tables as of certain dates. In addition to manipulating or deleting the data in these tables, we also had the ability to create private synonyms for each object. This would allow us to assign aliases for each table; thereafter any references to such aliases would point to the table of our choosing. For instance, if the user owned table X, and we created an alias of X for table Z, the next time the user writes a query referring to table X, the user would actually be querying against table Z because of the synonym we created. A user would not be aware that the synonym was created. Private synonyms take precedence over table names.

Effect: There is an increased risk of unauthorized access to the Core-CT back-end databases and possible manipulation or destruction of data.

Cause: The cause could not be determined.

Recommendation: The Core-CT security administration group should develop procedures to ensure that no database user account has the same password as the username. (See Recommendation 8.)

Agency Response: "Core-CT agrees with this recommendation. We will review existing user accounts and correct. The new user profile mentioned previously will prevent this from occurring."

Erroneous Creation of User Accounts

Background: The Core-CT system is comprised of applications and databases residing in both a development and production layer. The majority of state employees access the production layer. The development layer is used internally by Core-CT staff to develop and test customizations to the applications and data comprising production. Code changes are developed, tested, and approved within the development layer prior to being moved into production in an effort to fix any problems with new code or data prior to implementation of those changes.

Criteria: The National Institute on Standards and Technology Special Publication 800-53 recommends various configuration and change management (CM) controls. Control CM-03 states that "The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system."

Adequate controls should exist to prevent major system modifications from being migrated from development into production if those modifications contain errors.

Condition: Core-CT upgraded HRMS in November 2012. As part of this upgrade, Core-CT staff programmed a mass creation of user accounts to allow employees, including those who did not yet have a Core-CT account, to access some self-service functionality in Core-CT with respect to their payroll and benefits information.

During this process, they erroneously created new, additional usernames for 651 employees who already had usernames. Access to the new self-service functionality should have been assigned to their existing usernames.

In addition, 3,626 usernames were created for employees who had left state service at the time of the upgrade. These usernames were not assigned any access rights to the system, but still had no reason to be created and, as a result, they reside on the system in error.

Effect: 651 employees were given a second username in error.

3,626 usernames were created for terminated employees in error.

Cause: The development environment contained erroneous data which negatively impacted the developers' mass creation of user accounts. The resulting errors were not detected prior to implementation.

Recommendation: The Core-CT security administration group should strengthen controls over migration of code and data from development to production. Errors should be identified during development and testing and should be fixed prior to migration. (See Recommendation 9.)

Agency Response: "The creation of new User Accounts (Profiles) was automated for the purpose of having provisions in place for all employees to use Self-Service. The creation of User Profiles is triggered by the effective date or action date (whichever is greater) of a new hire's primary, active job row in HRMS Job Data and if the employee ID is not associated with a current Username. The code for this enhancement (Create new User Profile batch process) was migrated to production using the current change control processes in Core-CT.

Prior to the 9.1 upgrade, there were approximately 60,000 existing employees that did not have a User ID in Core-CT. Running the newly migrated batch process for this existing employee population within the 9.1 upgrade cutover timeframe was not a viable option. It was decided a one-time initial manual load using the same criteria as the Create New User Profile process would need to occur. After the 9.1 upgrade, any new hires would be picked up with a nightly batch process, incrementally. Lastly, security best practice dictates that User Security should never be migrated or overlay User Security in Production environment, as the Production environment represents the most current user security.

The 651 employees that were given a second username in error, was most likely due to the fact these employee's original (alpha) User Profiles did not include an Employee ID and/or were no longer valid. Employee IDs were not required in a User Profile at go-live in 2003. Later when this became a requirement, only active User Profiles were retrofitted with Employee IDs. Furthermore, it was decided to use Employee ID for all User IDs after the 9.1 upgrade. There is no policy in place that 'restricts' an employee to their original User ID; name changes and need for secondary IDs can occur. However, using the Employee ID as the naming standard for new User IDs after the 9.1 Upgrade and forward will be enforced at all possible times.

We question the 3,626 usernames created for terminated employees in error at the time of the upgrade. This could only have occurred if an employee status in Job Data was not current for an employee who has never had a Username in Core-CT. More information would be needed to clarify further.

Additionally, the Security Team does not 'delete' User Profiles in Core-CT. Inactivation of User Profiles includes locking user accounts, removing roles, row security and process profiles."

Auditors' Concluding Comments:

Regarding the 651 employees that were given a second username in error, both the prior and newly created username did have the employee's employee ID number on file. In addition, we were informed by e-mail that this issue occurred due to the usernames being created based off of erroneous or outdated data in the development environment.

Regarding the 3,626 usernames that were created for terminated employees at the time of the upgrade, while Core-CT staff might question the exact number, this issue was discussed during the Core-CT upgrade status meetings.

Asset Module Discrepancies

Criteria:

The State Property Control Manual dictates that personal property, having a value of one thousand dollars or more, be capitalized and personal property valued less than one thousand dollars not be capitalized. State agencies may request exceptions to this rule from the Office of the State Comptroller, which may accept or reject such requests.

The State of Connecticut currently uses asset and inventory modules in its financial system to account for its assets. Chapter 3 of the State Property Control Manual requires the annual submission of a CO-59 "Asset Management/Inventory Report/GAAP Reporting Form." The instructions on this form state that "Data generated from the [Core-CT] EPM queries can be replicated and if the values recorded on the CO-59 do not reconcile with Core-CT, [the] agency must provide a written explanation of the discrepancy in an attachment."

Condition:

As of the fiscal year ended June 30, 2012, there were 11,563 assets classified on Core-CT as capital or not capital in a way that conflicts with the capitalization criteria prescribed by the State Property Control Manual. Assets totaling $2,019,647 were not capitalized but should have been, and $3,389,521 of assets were capitalized but should not have been. An additional 24 assets were only partially capitalized while their full cost should have been capitalized, resulting in an understatement of $369,036. Net of both understatements and overstatements, the module overstated capital assets by $1,000,837.74 as of June 30, 2012.

In addition, as of the fiscal year ended June 30, 2012, there were six instances among three departments where the beginning balance of an asset category per the Core-CT asset module, plus additions, minus deletions, did not equal the ending balance per the Core-CT asset module. As of the fiscal year ended June 30, 2011, there were nine instances among five departments having the same condition.

Effect: The failure of agencies to capitalize assets on Core-CT where appropriate increases the likelihood that they will prepare and submit CO-59 Asset Management and Inventory Reports to the Office of the State Comptroller which contain the same errors, thereby causing financial statement errors.

Agencies are instructed to rely on figures produced by Core-CT queries when preparing their CO-59 Asset Management and Inventory reports. In the instances noted, such CO-59's are therefore based on inconsistent data and their accuracy is questionable. There is an increased likelihood that impacted agencies will report inaccurate asset balances to the Office of the State Comptroller, thereby causing additional financial statement errors.

Cause: The current financials system that Core-CT uses does not contain any application controls relative to a capitalization threshold whereby any asset over a certain amount is automatically capitalized by the system, or not capitalized if below that amount. Asset capitalization errors are not currently preventable through application controls.

We were informed that in some cases, Structured Query Language (SQL) scripts were run to transfer assets between parent and child agencies upon consolidations, and that development errors made during these processes sometimes led to balances between two dates not reconciling with the activity occurring in between. In other cases, the cause appears to be transactional errors by the agencies involved; however the specific circumstances of those errors cannot be determined.

Recommendation: Core-CT management should implement application controls relative to assets, where appropriate, upon their upgrade to the new financials system and should develop procedures to ensure that Core-CT asset balances reconcile with associated activity. (See Recommendation 10.)

Agency Response: "Core-CT does agree with the finding, however prior to PeopleSoft Version 9.1, there was no automated way to capitalize assets based upon a threshold cost. Agency personnel had to manually identify capital assets, which is the cause for the incorrect categorization of

assets. In March 2013, Core-CT upgraded to PeopleSoft version 9.1 which delivered new functionality to define and determine asset capitalization based on its cost or quantity. To address the potential for errors from manual capitalization, Core-CT enabled the Automatic Capitalization Threshold feature.

As part of the 9.1 upgrade, the 11,563 assets identified in the Audit (which included Real Property but should not have) and the 24 partially capitalized assets were all re-categorized correctly. With the implementation of this newly delivered functionality, Core-CT worked hand-in-hand with PeopleSoft to address issues with the new functionality and incorporate new procedures for agencies to ensure their assets were categorized accurately based upon all the adjustments that may occur.

At this time (FY2015), Core-CT is working on addressing incorrectly categorized assets due to bugs in the software encountered after the implementation of the newly delivered functionality. This should be completed by the end of FY2015. In addition, Core-CT is instituting a monthly reconciliation of participating agencies to ensure that the beginning balance of assets and all transactions during the month equal the ending balance, which will address the second finding.

As for the use of Structured Query Language (SQL) scripts, SQL scripts/updates are used only as a last resort for updating data if there is no system process to address the issue. In the case of transferring assets, SQL was not used to transfer assets; the delivered process of 'Mass Transfer' was used. However, due to several system bugs (which have been identified to PeopleSoft), SQL was used to update flags to complete the transfer process and adequately categorize the transferred assets."

Disaster Recovery Plan

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning controls (CP) in its special publication 800-53 (SP 800-53). Control CP-02, Contingency Plan, requires that the organization "reviews the contingency plan at an organization-defined frequency", and "updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing."

Condition: Our review disclosed that a single comprehensive disaster recovery plan does not exist for the Core-CT system. The Office of the State

Comptroller maintains several disparate disaster recovery plan documents that are specific to certain areas and operational teams, but has not integrated these documents into a single master plan.

The outcomes of Core-CT disaster recovery exercises are not documented in formal post write-ups, only minor details are recorded on change management forms.

Core-CT management have not yet conducted or planned to conduct a disaster recovery test whereby its disaster recovery hot site is used as the Core-CT system's primary infrastructure on a work day under conditions of normal load.

Effect: The Office of the State Comptroller's maintenance of several disaster recovery plan documents that are specific to layers of infrastructure and operational teams, in lieu of an integrated master plan, could result in a lack of coordination when attempting to carry out the procedures upon the occurrence of a disaster and negatively impact the state's ability to resume critical operations within a reasonable period of time or to ensure the completion of all required steps.

The lack of detailed documentation outlining the successes and failures of disaster recovery tests – including an analysis of procedural strengths and weaknesses – may inhibit potential improvements to the agency's current processes from being made.

It is uncertain whether the Core-CT system could operate from the disaster recovery hot site under normal load by state employees on a work day.

Cause: We were unable to determine the causes of these deficiencies.

Recommendation: Core-CT should develop and completely test a single comprehensive disaster recovery plan for the Core-CT system with detailed post write-ups to be completed after each test. (See Recommendation 11.)

Agency Response: "Core-CT agrees with this recommendation and will improve the disaster recovery documentation as time permits. As was noted in the finding, the system recovery procedures are documented and the recovery site has been successfully tested several times."

Lack of Service Level Agreement

Criteria: The National Institute on Standards and Technology (NIST) recommends various contingency planning (CP) controls in Special

Publication 800-53. Control CP-06, Alternate Storage Site, states that an organization should establish an alternate storage site "including any necessary agreements to permit the storage and recovery of information system backup information."

Condition: No agreement exists between the Office of the State Comptroller and the provider of the disaster recovery hot site for the Office of the State Comptroller to use its location as a Core-CT disaster recovery hot site, despite their current use of it as such.

Effect: The Office of the State Comptroller is vulnerable to the risk that the provider of the disaster recovery hot site may at any time decide that it does not want Core-CT hardware in its datacenter, or may reduce the amount of physical space available for such hardware.

Cause: We were informed that a memorandum of understanding regarding the terms of the Comptroller's use of the provider's datacenter was drafted during project implementation but was never signed by both parties. Other causes could not be identified.

Recommendation: A formal agreement outlining the terms of the Office of the State Comptroller's use of the provider's datacenter as a Core-CT disaster recovery hot site should be written and entered into. (See Recommendation 12.)

Agency Response: "Core-CT agrees with this recommendation and will pursue a formal agreement. However, since the disaster recovery site is a State facility, the risks highlighted above are diminished."

Background Checks

Criteria: The National Institute of Standards and Technology (NIST) recommends various personnel security controls (PS) in its special publication 800-53 (SP 800-53).

Control PS-03, Personnel Screening, requires that the organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to organizational defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.

Condition: We interviewed personnel from the Office of the State Comptroller responsible for Core-CT staffing and determined that OSC does 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 or alteration.

Cause: Although a specific cause was not identified, it appears that the agency does not think that background checks are required.

Recommendations: Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT system. (See recommendation 13.)

Agency Response: "While NIST recommends various personnel security controls, Connecticut General Statutes address the limitations and restrictions of using "background" information--particularly arrest and conviction histories--in state employment decision-making. Core-CT will study the feasibility and legal and practical requirements of requiring background checks."

RECOMMENDATIONS

Our prior report on the Core-CT General Controls Audit completed in July 2007, contained eighteen recommendations**.**

Status of Prior Audit Recommendations:

- 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. Our current audit showed that the recommendation was effectively implemented. This recommendation is not being repeated.

- 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. Our current audit showed that the recommendation was effectively implemented. This recommendation is not being repeated.

- 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. Our current audit showed significant improvement, with only one minor exception. This recommendation is not being repeated.

- A written service-level agreement detailing the responsibilities of the Core-CT Project team and DOIT should be developed and implemented. This recommendation is being repeated in an amended form. (See recommendation 12.)

- 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. This recommendation is being repeated in an amended form. (See recommendation 11.)

- 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. The MOU that created the Steering Committee in no long in effect, therefore eliminating the requirement for committee to meet. This recommendation is not being repeated.

- Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT project. This recommendation is being repeated in an amended form. (See recommendation 13.)

- 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. The Core-CT Policy Board was never created and OSC has indicated that they will present legislation to have the statutory requirement eliminated. This recommendation is not being repeated.

Current Audit Recommendations:

1. **The Core-CT security administration group should take steps to ensure that permission lists are always assigned appropriate sign-on schedules.**

   Comments:

   Sign-on schedules with 24/7 access were inadvertently assigned to other permission lists that were associated with users' default sign-on roles. As a result, all Core-CT users were able to access the system 24/7 at the time of our testing.

2. **The Core-CT security administration group should take steps to ensure that password controls are properly configured in the back-end production databases.**

   Comments:

   Password policies were not properly configured in the back-end production databases.

3. **Core-CT personnel should strengthen its controls over segregation of duties conflicts within the Core-CT system and develop a means of tracking any exceptions or waivers that they have granted to certain employees or departments.**

   Comments:

   Although, the Core-CT Role Handbooks allow for expectations to the segregation of duties policy when an agency provides written justification and shows that compensating controls are in place, the Core-CT personnel do not maintain logs of which employees have been granted an exception or waiver.

4. **The Core-CT security administration group should develop procedures to ensure that all database application controls are used where appropriate and configured properly to prevent unauthorized access to confidential information.**

   Comments:

   Some employees had access to confidential employee information that was not necessary for their position. The lack of strong controls in this area leaves state employees vulnerable to having their personal information accessed by employees of

other departments who have no need to access such information.

5. **The Core-CT security administration group should develop procedures to ensure a periodic review of who has access the databases behind the Core-CT system and ensure that user accounts are deactivated in a timely manner.**

   Comments:

   We found that some individuals who were previous consultants or separated state employees had active access to the database.

6. **The Core-CT security administration group should develop procedures to ensure a periodic review of what access each database user has and to ensure that access levels are appropriate and consistent with their job duties.**

   Comments:

   We found that there are no formal procedures and forms to be completed for requesting, granting or modifying access to the Core-CT back-end databases.

7. **The Core-CT security administration group should develop procedures to ensure that no single database user account, with the exception of system usernames used by database administrators, is shared by more than one individual, and that passwords never match their associated usernames.**

   Comments:

   We found that multiple employees of the Office of the State Comptroller (OSC) used a single database user account and the password for this account was identical to the username.

8. **The Core-CT security administration group should develop procedures to ensure that no database user account has the same password as the username.**

   Comments:

   We found some database accounts had the same password as the username.

9. **The Core-CT security administration group should strengthen controls over migration of code and data from development to production. Errors should be identified during development and testing and should be fixed prior to migration.**

   Comments:

   Core-CT upgraded HRMS a mass creation of user accounts occurred so all employees could access some self-service functionality. During this process, a

significant number of erroneous accounts were created and migrated to the production environment.

10. **Core-CT management should implement application controls relative to assets, where appropriate, upon their upgrade to the new financials system and should develop procedures to ensure that Core-CT asset balances reconcile with associated activity.**

    Comments:

    We found that some assets classified on Core-CT were not classified correctly as capital or not capital in a way that complies with the criteria prescribed by the State Property Control Manual. In addition, there were instances in which the balances of an asset category were not accurate.

11. **Core-CT should develop and completely test a single comprehensive disaster recovery plan for the Core-CT system, with detailed post write-ups to be completed after each test.**

    Comments:

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

12. **A formal agreement outlining the terms of the Office of the State Comptroller's use of the provider's datacenter as a Core-CT disaster recovery hot site should be written and entered into.**

    Comments:

    No service level agreement exists between the Core-CT Project team and the Department of Administrative Services – Bureau of Enterprise Systems and Technology (BEST) covering the services provided by BEST's data center.

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

    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 cooperation and courtesies extended to our representatives by the personnel of the Office of the State Comptroller and the Department of Administrative Services during the course of the examination.

Bruce C. Vaughan
Principal Auditor

Approved:

John C. Geragosian
Auditor of Public Accounts

Robert M. Ward
Auditor of Public Accounts